DOCKET

SUPREME COURT
OF THE UNITED STATES

No. 13-132
Title: David Leon Riley, Petitioner
v.
California
Docketed: July 31, 2013
Lower Ct: Court of Appeal of California, Fourth Appellate District, Division One
Case Nos.: (D059840)
Decision Date: February 8, 2013
Discretionary Court
Decision Date: May 1, 2013
Questions Presented

~~Date~~~	~~~~~~~Proceedings and Orders~~~~~~~~~~~~~~~~~~~~
Jul 30 2013	Petition for a writ of certiorari filed. (Response due August 30, 2013)
Aug 12 2013	Waiver of right of respondent California to respond filed.
Aug 15 2013	Consent to the filing of amicus curae briefs, in support of either party or of neither party, received from counsel for the petitioner.
Aug 21 2013	DISTRIBUTED for Conference of September 30, 2013.
Aug 30 2013	Brief amici curiae of Center for Democracy & Technology and Electronic Frontier Foundation filed. (Distributed)
Aug 30 2013	Brief amicus curiae of Constitutional Accountability Center filed.
Aug 30 2013	Brief amicus curiae of National Association of Criminal Defense Lawyers filed.
Sep 3 2013	Response Requested . (Due October 3, 2013)
Sep 27 2013	Brief of respondent California in opposition filed.
Oct 16 2013	Reply of petitioner David Leon Riley filed.
Nov 20 2013	DISTRIBUTED for Conference of December 6, 2013.
Dec 3 2013	Record Requested .
Dec 23 2013	Record received. California Court of Appeal for the Fourth Appellate District and San Diego Superior Court (1 box)
Dec 31 2013	DISTRIBUTED for Conference of January 17, 2014.
Jan 17 2014	Petition GRANTED limited to the following question: Whether evidence admitted at petitioner's trial was obtained in a search of petitioner's cell phone that violated petitioner's Fourth Amendment rights.
Feb 11 2014	SET FOR ARGUMENT ON Tuesday, April 29, 2014
Feb 18 2014	Consent to the filing of amicus curiae briefs, in support of either party or of neither party, received from counsel for the petitioner.

Feb 19 2014	Consent to the filing of amicus curiae briefs, in support of either party or of neither party, rece8ved from counsel for the respondent.
Mar 3 2014	Joint appendix filed. (Statement of costs filed.)
Mar 3 2014	Brief of petitioner David Leon Riley filed.
Mar 7 2014	Brief amici curiae of Criminal Law Professors in support of private parties filed. VIDED. (Distributed)
Mar 7 2014	Brief amici curiae of American Civil Liberties Union, et al. filed. (Distributed)
Mar 10 2014	CIRCULATED.
Mar 10 2014	Brief amici curiae of American Library Assciation, and The Internet Archive in support of Riley and Wurie filed. VIDED. (Distributed)
Mar 10 2014	Brief amicus curiae of Constitutional Accountability Center in support of Riley and Wurie filed. VIDED.
Mar 10 2014	Brief amici curiae of Center for Democracy & Technology, and Electronic Frontier Foundation in support of Riley and Wurie filed. VIDED. (Distributed)
Mar 10 2014	Brief amicus curiae of National Association of Criminal Defense Lawyers, et al. filed. (Distributed)
Mar 10 2014	Brief amicus curiae of DKT Liberty Project filed. (Distributed)
Mar 10 2014	Brief amici curiae of Electronic Privacy Information Center, et al. filed. (Distributed)
Mar 10 2014	Brief amici curiae of National Press Photographers Association, et al. filed. VIDED. (Distributed)
Mar 10 2014	Brief amici curiae of Professors Charles E. MacLean & Adam Lamparello filed. (Distributed)
Mar 10 2014	Brief amicus curiae of The Cato Institute filed. (Distributed)
Apr 2 2014	Brief of respondent California filed. (Distributed)
Apr 9 2014	Brief amicus curiae of United States filed. (Distributed)
Apr 9 2014	Brief amici curiae of Association of State Criminal Investigative Agencies, et al. filed. (Distributed)
Apr 9 2014	Brief amici curiae of Arizona, et al. filed. (Reprinted) (Distributed)
Apr 10 2014	Motion of the Solicitor General for leave to participate in oral argument as amicus curiae and for divided argument filed.
Apr 18 2014	Motion of the Solicitor General for leave to participate in oral argument as amicus curiae and for divided argument GRANTED.
Apr 22 2014	Reply of petitioner David Leon Riley filed. (Distributed)
Apr 29 2014	Argued. For petitioner: Jeffrey L. Fisher, Stanford, Cal. For respondent: Edward C. DuMont, Solicitor General, San Francisco, Cal.; and Michael R. Dreeben, Deputy Solicitor General, Department of Justice, Washington, D. C. (for United States, as amicus curiae.)
Jun 25 2014	Judgment REVERSED and case REMANDED. Roberts, C. J., delivered the opinion of the Court, in which Scalia, Kennedy, Thomas, Ginsburg, Breyer, Sotomayor, and Kagan, JJ., joined. Alito, J., filed an opinion concurring in part and concurring in the judgment. VIDED with No. 13-212.
Jul 28 2014	MANDATE ISSUED.
Jul 28 2014	Record returned for Court of Appeal of California, Fourth Appellate District, Division One.

PETITION FOR WRIT OF CERTIORARI

RECORD AND BRIEFS

13-132

Supreme Court, U.S.
FILED
JUL 30 2013
OFFICE OF THE CLERK

No. 13-___

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Petition for a Writ of Certiorari
to the California Court of Appeal, Fourth District

PETITION FOR A WRIT OF CERTIORARI

Patrick Morgan Ford
ATTORNEY AT LAW
1901 First Avenue
Suite 400
San Diego, CA 92101

Kevin K. Russell
GOLDSTEIN &
RUSSELL, P.C.
5225 Wisconsin Ave., NW
Suite 404
Washington, DC 20036

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@law.stanford.edu

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

QUESTION PRESENTED

Whether or under what circumstances the Fourth Amendment permits police officers to conduct a warrantless search of the digital contents of an individual's cell phone seized from the person at the time of arrest.

TABLE OF CONTENTS

QUESTION PRESENTED i

PETITION FOR A WRIT OF CERTIORARI 1

OPINIONS BELOW 1

JURISDICTION 1

RELEVANT CONSTITUTIONAL PROVISION 1

STATEMENT OF THE CASE 1

REASONS FOR GRANTING THE WRIT 7

I. Federal And State Courts Are Openly Divided Over Whether The Fourth Amendment Permits Police Officers To Search The Digital Contents Of An Arrestee's Cell Phone Incident To Arrest. 7

A. Background 7

B. The Conflict 11

II. The Propriety Of Cell Phone Searches Incident To Arrest Should Be Resolved Now. 14

A. The Issue Greatly Affects Personal Privacy And Day-To-Day Police Operations. 14

B. Additional Percolation Would Not Aid This Court's Consideration Of The Issue. 16

III. This Case Is An Excellent Vehicle For The Court To Resolve The Conflict 19

IV. The Fourth Amendment Prohibits Searching The Digital Contents Of A Cell Phone Incident To Arrest. 21

A. Neither Of The *Chimel* Rationales For Searches Incident To Arrest Is Present Here. 22

B. The Profound Privacy Concerns Related To Cell Phones Make It Unreasonable To Search Them Without Warrants. 25

CONCLUSION 28

APPENDIX

Court of Appeal's Decision 1a

Denial of Discretionary Review 24a

California Supreme Court's opinion in *People v. Diaz* 25a

TABLE OF AUTHORITIES

Page(s)

Cases

Arizona v. Gant, 556 U.S. 332 (2009) ..... *passim*

Atwater v. City of Lago Vista, 532 U.S. 318 (2001) 14

Chimel v. California, 395 U.S. 752 (1969) ..... *passim*

Commonwealth v. Phifer, 979 N.E.2d 210 (Mass. 2012) 12

Diaz v. California, 132 S. Ct. 94 (2011) 6

Hawkins v. State, 723 S.E.2d 924 (Ga. 2012) 12

Missouri v. McNeely, 133 S. Ct. 1552 (2013) 23

New York v. Belton, 453 U.S. 454 (1981) 15, 26, 27

Newhard v. Borders, 649 F. Supp. 2d 440 (W.D. Va. 2009) 11

People v. Diaz, 244 P.3d 501 (Cal. 2011), *cert denied*, 132 S. Ct. 94 (2011) ..... *passim*

People v. Nottoli, 130 Cal. Rptr. 3d 884 (Cal. Ct. App. 2011) 15

Sibron v. New York, 392 U.S. 40 (1968) 22

Silvan W. v. Briggs, 309 Fed. App'x 216 (10th Cir. 2009) 12

Smallwood v. State, 113 So. 3d 724 (Fla. 2013) ..... *passim*

State v. Boyd, 992 A.2d 1071 (Conn. 2010), *cert. denied*, 131 S. Ct. 1474 (2011) 12

State v. Carroll, 778 N.W.2d 1 (Wis. 2010) 13

State v. Smith, 920 N.E.2d 949 (Ohio 2009), *cert. denied*, 131 S. Ct. 102 (2010) 13, 23, 26

Stoner v. California, 376 U.S. 483 (1964) 21

Thornton v. United States, 541 U.S. 615 (2004) 22

Trupiano v. United States, 334 U.S. 699 (1948) 21

United States v. Chadwick, 433 U.S. 1 (1977) ..... *passim*

United States v. Curtis, 635 F.3d 704 (5th Cir. 2011) 24

United States v. Edwards, 415 U.S. 800 (1974) 20, 21

United States v. Finley, 477 F.3d 250 (5th Cir. 2007), *cert. denied*, 549 U.S. 1353 (2007) 12, 19

United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) ..... *passim*

United States v. Jones, 132 S. Ct. 945 (2012) 17, 28

United States v. Knights, 534 U.S. 112 (2001) 27

United States v. Murphy, 552 F.3d 405 (4th Cir. 2009), *cert. denied*, 129 S. Ct. 2016 (2009) 12, 19

United States v. Robinson, 414 U.S. 218 (1973) ..... *passim*

United States v. Ross, 456 U.S. 798 (1982) 26

United States v. Wurie, __ F.3d __, 2013 WL 2129119 (1st Cir. May 17, 2013) ..... *passim*

Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) 27

Wyoming v. Houghton, 526 U.S. 295 (1999) 27

Constitutional Provision

U.S. Const., amend. IV ..... *passim*

Statutes

28 U.S.C. § 1257(A) 1

Cal. Penal Code § 186.22(b)(4)(B) 5

Cal. Penal Code § 246 5

Other Authorities

Anderson, Leanne, People v. Diaz: *Warrantless Searches of Cellular Phones, Stretching the Search Incident to Arrest Exception Beyond the Breaking Point*, 39 W. St. U.L. Rev. 33 (2011) 18

Brown, Edmund G., Letter from Edmund G. Brown Jr., Governor, to Members of the California State Senate (Oct. 10, 2011) 6

Cal. Senate Bill 914 (2011) 6

Clark, M. Wesley, *Searching Cell Phones Seized Incident to Arrest*, FBI L. Enforcement Bull. (Feb. 2009) 14

Dwyer, Terrence P., *Cell Phones, Privacy, and the Fourth Amendment*, PoliceOne.com (Aug. 10, 2012) 16

Gershowitz, Adam M., *The iPhone Meets the Fourth Amendment*, 56 UCLA L. Rev. 27 (2008) 17

Kerr, Orin S., *Foreword: Accounting for Technological Change*, 36 Harv. J. L. & Pub. Pol'y 403 (2013) 17

Kish, Byron, Comment, *Cellphone Searches: Works Like a Computer, Protected Like a Pager?*, 60 Cath. U. L. Rev. 445 (2011) 18

Knott, Jana L., Note, *Is There an App for That? Reexamining the Doctrine of Search Incident to Arrest in the Context of Cell Phones*, 35 Okla. City U. L. Rev. 445 (2010).....18

Maclean, Charles R., *But, Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to* Chimel *Justifications for Cell Phone Memory Searches Incident to Arrest*, 6 Fed. Cts. L. Rev. 37 (2012).....17

Mass. Mun. Police Training, Legal Update: *Searching Cell Phones Incident to Arrest* (2012) 16

Orso, Matthew E., *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L. Rev. 183 (2010).....17

Oxton, Chelsea, Note, *The Search Incident to Arrest Exception Plays Catch Up: Why Police May No Longer Search Cell Phones Incident to Arrest Without a Warrant*, 43 Creighton L. Rev. 1157 (2010).....18

Park, Eunice, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-to-Arrest Exception to the Cell Phone as "Hybrid,"* 60 Drake L. Rev. 429 (2012).....18

Snyder, Ashley B., Comment, *The Fourth Amendment and Warrantless Cell Phone Searches: When Is Your Cell Phone Protected?*, 46 Wake Forest L. Rev. 155 (2011)...18

Stewart, Ben E., Note, *Cell Phone Searches Incident to Arrest: A New Standard Based on* Arizona v. Gant, 99 Ky. L.J. 579 (2010-2011).....18

U.S. Dep't of Justice, Computer Crime & Intellectual Prop. Section, Criminal Div., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009).....16

Warfield, J. Patrick, Note, *Putting a Square Peg in a Round Hole: The Search-Incident-to-Arrest Exception and Cellular Phones,* 34 Am. J. Trial Advoc. 165 (2010) 18

Woyke, Elizabeth, *Debate Over Warrantless Cellphone Searches Heats Up,* Forbes (Sept. 7, 2011).....26

PETITION FOR A WRIT OF CERTIORARI

Petitioner David Leon Riley respectfully petitions for a writ of certiorari to review the judgment of the California Court of Appeal, Fourth District, Division One, in Case No. D059840.

OPINIONS BELOW

The opinion of the California Court of Appeal (Pet. App. 1a) is unpublished but can be found at 2013 WL 475242. The order of the California Supreme Court denying review (Pet. App. 24a) is unpublished. The relevant trial court proceedings and order are unpublished.

JURISDICTION

The California Supreme Court denied review on May 1, 2013. Pet. App. 24a. This Court has jurisdiction pursuant to 28 U.S.C. § 1257(A).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment states in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."

STATEMENT OF THE CASE

1. Early in the morning on August 22, 2009, the police pulled over petitioner David Riley, a local college student, who was driving his Lexus near his home in San Diego. The officer who initiated the stop, Charles Dunnigan, told petitioner that he had pulled him over for having expired tags. Pet. App. 3a, 5a. Officer Dunnigan soon learned that petitioner

was driving with a suspended license and thus decided to impound petitioner's car.

At the inception of an impound, San Diego Police Department policy requires officers to conduct an inventory search of the vehicle in order to document its contents. Pet. App. 5a. Officer Dunnigan called in another officer to assist with this task. Tr. 112. During the inventory search, the officers discovered two firearms under the car's hood. Pet. App. 3a, 6a. Based on this discovery, Officer Dunnigan placed petitioner under arrest for carrying concealed and loaded weapons. Pet. App. 6a.

During the arrest, Officer Dunnigan seized petitioner's cell phone from his person. Pet. App. 15a.[1] The phone was a Samsung Instinct M800 "smartphone" – a touch-screen device designed to compete with Apple's iPhone, capable of accessing the internet, capturing photos and videos, and storing both voice and text messages, among other functions. *Samsung Instinct Touchscreen Cell Phone: Features*, Samsung, http://www.samsung.com/us/mobile/cell-phones/SPH-M800ZKASPR-features (last visited July 28, 2013).

Upon seizing petitioner's phone, officers performed two separate, warrantless searches of its

---

[1] Some testimony presented at trial suggested that petitioner's phone might have been sitting on the seat of his car instead of on his person at the time of arrest. Pet. App. 15a. But the trial court found that "the cell phone . . . was on [Riley's] person at the time of the arrest," and the California Court of Appeal treated that finding as binding for purposes of appeal. *Id.* Accordingly, petitioner proceeds here on the basis of that finding as well.

digital contents. First, Officer Dunnigan scrolled through the phone's contents at the scene. He noticed that some words (apparently in text messages and the phone's contacts list) normally beginning with the letter "K" were preceded by the letter "C." Pet. App. 6a; Tr. at 114-15. Officer Dunnigan believed that the "CK" prefix referred to "Crip Killers," a slang term for members of a criminal gang known as the "Bloods." Tr. at 114-15.

The second search of petitioner's phone took place hours later at the police station. After conducting an interrogation in which petitioner was nonresponsive, Detective Duane Malinowski, a detective specializing in gang investigations, went through petitioner's cell phone. The detective searched through "a lot of stuff" on the phone "looking for evidence." Tr. 176, 193. Detective Malinowski found several photographs and videos that suggested petitioner was a member of a gang. Pet. App. 4a, 6a-7a. He also found a photo of petitioner with another person posing in front of a red Oldsmobile that the police suspected had been involved in a prior shooting.

In the shooting incident, three individuals had reportedly fired several shots at a passing car before fleeing in a red Oldsmobile. The police believed the shooting was gang related. After finding the photos on petitioner's phone indicating that he owned a red Oldsmobile and that he was connected to gang activity, and after ballistics testing suggested that the firearms seized during petitioner's traffic stop were used in the shooting incident, law enforcement came to believe that petitioner had been involved in that incident.

2. The State ultimately charged petitioner and two others with shooting at an occupied vehicle, attempted murder, and assault with a semiautomatic firearm.[2] The State also alleged that petitioner committed these crimes for the benefit of a criminal street gang – an allegation that not only rendered evidence of petitioner's alleged membership in a nefarious street gang admissible (and, indeed, highly relevant) at trial but also exposed him under California law to significantly enhanced sentences. The two co-defendants eventually pleaded guilty to involvement in the crime, but petitioner insisted on his innocence.

Prior to trial, petitioner moved to suppress all of the evidence the police had obtained during the searches of his cell phone. Tr. at 269-70. As is pertinent here, petitioner argued that the search of his cell phone violated the Fourth Amendment because it was performed without a warrant and without any exigency otherwise justifying the search. Tr. at 269-70. The trial judge rejected this argument, ruling that the searches were legitimate searches incident to arrest. Pet. App. 7a-8a.

The trial ended in a hung jury, but the State elected to retry petitioner. During the second trial (as at the first), none of the State's four eyewitnesses could identify petitioner as one of the shooters. The

---

[2] The State separately charged petitioner in conjunction with the traffic stop with carrying a concealed firearm in a vehicle, carrying a loaded firearm, and receiving stolen property. Petitioner pleaded guilty to all three charges and was sentenced to four years in prison. Those convictions are not at issue here.

State, therefore, relied on circumstantial evidence to connect petitioner to the crime. Among other things, the State showed the jury the photo of petitioner posing in front of the Oldsmobile with one of the co-defendants. In addition, the State presented videos from petitioner's cell phone showing street boxing fights involving both co-defendants, in which petitioner could be heard in the background encouraging the co-defendants and shouting gang-related comments.

The jury convicted petitioner on all three charges. Pursuant to California law, the trial court stayed petitioner's sentences on the two convictions carrying lesser sentences, activating petitioner's sentence only on the conviction that carried the longest sentence, in this case shooting at an occupied vehicle. Without the gang enhancement, this crime is punishable by a maximum of seven years in prison. Cal. Penal Code § 246. With the gang enhancement, however, petitioner's conviction for shooting at an occupied vehicle required the court to sentence him to fifteen years to life in prison. Pet. App. 1a; *see also* Cal. Penal Code § 186.22(b)(4)(B).

3. While petitioner's case was proceeding to trial, the California Supreme Court decided *People v. Diaz*, 244 P.3d 501 (Cal. 2011). In that decision, which is reproduced at Pet. App. 25a-65a, the California Supreme Court held by a 5-2 vote that the Fourth Amendment's search-incident-to-arrest doctrine permits the police to search a cell phone (even some time later at the stationhouse) whenever the phone is "immediately associated with [the arrestee's] person" at the time of the arrest. Pet. App. 33a-34a. The majority acknowledged that its holding deepened a

conflict on the issue among federal courts of appeals and state supreme courts. *Id.* 47a n.17. But the majority maintained that only this Court has the power to distinguish searching the digital contents of a cell phone from this Court's prior decisions allowing police officers to search the physical contents of ordinary containers incident to arrest. *Id.* 47a.

Mr. Diaz filed a petition for a writ of certiorari. Shortly thereafter, the California Legislature passed a bill requiring the police to obtain a search warrant before searching the contents of any "'portable electronic devices,' including cellular telephones." Supplemental Br. in Opp. 1, *Diaz v. California*, 132 S. Ct. 94 (2011) (No. 10-1231), 2011 WL 4366007, at *1 (describing Senate Bill 914 (2011)). After the State brought this bill to this Court's attention, *see id.*, the Court, at the State's urging, denied review. 132 S. Ct. 94 (2011). One week later, California Governor Jerry Brown vetoed the state legislature's bill, stating that the "courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections." Letter from Edmund G. Brown Jr., Governor, to Members of the California State Senate (Oct. 10, 2011), *available at* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0901-0950/sb_914_vt_20111009.html.

4. The California Court of Appeal affirmed petitioner's convictions. As is relevant here, the court held that "*Diaz* controls the present case" because the cell phone was "immediately associated with [petitioner's] person" at the time of his arrest. Pet. App. 15a.

5. Petitioner sought discretionary review in the California Supreme Court. As is pertinent here, he

renewed his argument that the warrantless searches of his cell phone violated the Fourth Amendment. Pet. for Review at 13-20. The California Supreme Court denied review without comment. Pet. App. 24a.

REASONS FOR GRANTING THE WRIT

Federal courts of appeals and state courts of last resort are openly and intractably divided over whether the Fourth Amendment permits the police to search the digital contents of an arrestee's cell phone incident to arrest. This issue is manifestly significant. It also has had more than sufficient time to percolate. This Court should use this case – which presents the issue in the context of a modern "smartphone" and a particularly comprehensive fact pattern – to resolve the conflict and to hold that the Fourth Amendment prohibits such searches without a warrant.

I. Federal And State Courts Are Openly Divided Over Whether The Fourth Amendment Permits Police Officers To Search The Digital Contents Of An Arrestee's Cell Phone Incident To Arrest.

A. Background

The conflict over whether the Fourth Amendment permits police officers to search the digital contents of cell phones incident to arrest arises from (1) seemingly divergent threads in this Court's precedent and (2) disagreement over the import of qualitative differences between cell phones and traditional physical containers that might be seized incident to arrest.

1. The modern framework for analyzing the search-incident-to-arrest exception to the warrant requirement emanates from *Chimel v. California*, 395 U.S. 752 (1969). In that case, this Court explained that, in order to "seize weapons and to prevent the destruction of evidence," the Fourth Amendment permits police officers to search "the arrestee's person" and "the area into which an arrestee might reach" while being arrested. *Id.* at 763-64 (internal quotation marks and citation omitted).

This Court elaborated on the search-incident-to-arrest doctrine in *United States v. Robinson*, 414 U.S. 218 (1973). There, this Court upheld an officer's search of a crumpled cigarette package found on the defendant's person during his arrest. Rejecting the argument that the search was unlawful because the package was unlikely to contain any weapon or evidence related to the crime of arrest, this Court reasoned that searches incident to arrest do not depend on "the probability in a particular arrest situation that weapons or evidence would in fact be found." *Id.* at 235. This Court also stated – perhaps even more categorically – that "[i]t is the fact of the lawful arrest which establishes the authority to search." *Id.*

At the same time, this Court has indicated that a lawful arrest does not always allow the police to search items they seize during that arrest. In *United States v. Chadwick*, 433 U.S. 1 (1977), this Court held that the Fourth Amendment did not allow officers to search a locked footlocker they had seized from a person while arresting him. This Court reasoned that once the officers had "exclusive control" over the footlocker, "there [was] no longer any danger

that the arrestee might gain access to the property to seize a weapon or destroy evidence." *Id.* at 15. More recently, this Court held that the search of an arrestee's vehicle incident to arrest violates the Fourth Amendment when the arrestee is handcuffed in the patrol car at the time of the search. *Arizona v. Gant*, 556 U.S. 332 (2009). Applying *Chimel*, this Court explained that where "there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply." *Id.* at 339.

2. Courts across the country are now "struggl[ing] to apply [this] Court's search-incident-to-arrest jurisprudence" – a set of legal rules largely developed decades ago, before the digital era – to the question whether the Fourth Amendment permits warrantless "search[es] of data on a cell phone seized from the person." *United States v. Wurie*, ___ F.3d ___, 2013 WL 2129119, at *4 (1st Cir. May 17, 2013).

Modern cell phones provide ready access to a vast array of personal data, and are distinct from the types of possessions – such as cigarette packages and footlockers – this Court has previously considered. For one thing, while physical containers face obvious space-related constraints, cell phones are capable of storing a virtually limitless amount of information in a single, compact device. Accordingly, individuals can carry exponentially larger quantities of personal information on their person than they ever could prior to the advent of cell phones.

Additionally, cell phones are capable of storing, recording, and accessing private information in a

variety of forms. Typical "smartphones" contain, for example, a digital rolodex of contacts, several months or even years of past text and email correspondence, and detailed appointment calendars. Indeed, "[e]ven the dumbest of modern cell phones gives the user access to large stores of information. For example, the 'TracFone Prepaid Cell Phone,' sold by Walgreens for $14.99, includes a camera, MMS (multimedia messaging service) picture messaging for sending and receiving photos, video, etc., mobile web access, text messaging, voicemail, call waiting, a voice recorder, and a phonebook that can hold 1000 entries." *United States v. Flores-Lopez*, 670 F.3d 803, 806 (7th Cir. 2012).

Beyond the advanced capabilities of the phones themselves, modern cell phones incorporate computers that allow individuals to access the internet, presenting additional privacy concerns. Thus, a search incident to arrest could, at the touch of a button, become a search of private and confidential information such as medical records, banking activity, and work-related emails. *See Smallwood v. State*, 113 So. 3d 724, 729 (Fla. 2013).[3] The contents of a person's cell phone can also contain intimate details and video of people's private lives, potentially exposing them to extreme embarrassment or worse. *See, e.g., Newhard v. Borders*, 649 F. Supp.

---

[3] *See also* Maeve Duggan & Lee Rainie, Pew Research Ctr.'s Internet & Am. Life Project, Cell Phone Activities 2012, at 2 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.25.pdf (noting that 29% of cell phone owners use their phones for online banking, and 31% access medical information).

2d 440, 443-44 (W.D. Va. 2009) (noting that after the police arrested a school teacher for a DUI, they searched his cell phone and found sexually explicit photos of him and his girlfriend and then shared the photos with other officers and members of the public).

B. The Conflict

The struggle to apply this Court's precedent to the unique technological capabilities of cell phones has divided federal courts of appeals and state courts of last resort over whether police officers may search the digital contents of a cell phone incident to arrest. At least six courts hold that the Fourth Amendment permits such searches, while at least three others hold that it does not.

1. Three federal courts of appeals and three state courts of last resort have concluded that the Fourth Amendment permits police officers to search all or at least some of the digital contents of a cell phone incident to arrest. Three courts, including the California Supreme Court, rely on *Robinson* to hold that such searches are categorically permitted, reasoning "there is no legal basis" for distinguishing the digital contents of a cell phone from any other item that the police may discover and seize from a person incident to arrest. *People v. Diaz*, 244 P.3d 501, 510 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011) (reproduced at Pet. App. 43a); *United States v. Murphy*, 552 F.3d 405, 411-12 (4th Cir. 2009), *cert. denied*, 129 S. Ct. 2016 (2009); *United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007), *cert. denied*, 549 U.S. 1353 (2007). Accordingly, these

courts hold that police officers may always search any digital contents within a cell phone without seeking a warrant.[4]

Three other courts have held that police may search certain digital files within cell phones incident to arrest, without opining whether every type of file is open to such inspection. *United States v. Flores-Lopez*, 670 F.3d 803, 809-10 (7th Cir. 2012) (search to obtain the cell phone's number); *Commonwealth v. Phifer*, 979 N.E.2d 210, 216 (Mass. 2012) (search of recent call list); *Hawkins v. State*, 723 S.E.2d 924, 926 (Ga. 2012) (search to obtain text messages that was limited "'as much as is reasonably practicable by the object of the search'") (internal quotation marks and citation omitted).

2. In direct contrast, one federal court of appeals and at least two state courts of last resort have held that the Fourth Amendment forbids police officers from searching any digital contents of a cell phone incident to an arrest without a warrant. *See United States v. Wurie*, ___ F.3d ___, 2013 WL 2129119, at *11 (1st Cir. May 17, 2013); *Smallwood v. State*, 113 So. 3d 724, 735-36 (Fla. 2013); *State v. Smith*, 920 N.E.2d 949, 956 (Ohio 2009), *cert. denied*, 131 S. Ct.

---

[4] The Tenth Circuit, in an unpublished opinion, has also endorsed the categorical proposition that "the permissible scope of a search incident to arrest includes the contents of a cell phone found on the arrestee's person." *Silvan W. v. Briggs*, 309 Fed. App'x 216, 225 (10th Cir. 2009). Furthermore, the Supreme Court of Connecticut has allowed cell phone searches in the context of the automobile exception, using reasoning that appears to apply with equal force in the search-incident-to-arrest context. *See State v. Boyd*, 992 A.2d 1071, 1089 & n.17 (Conn. 2010), *cert. denied*, 131 S. Ct. 1474 (2011).

102 (2010).[5] Two of these three decisions (*Wurie* and *Smallwood*) post-date this Court's earlier denials of certiorari on this issue and thus cement the conflict.

In the view of these courts, it "defies logic and common sense in this digital and technological age" to equate the contents of a cell phone with the kinds of physical objects at issue in *Robinson* and other cases, *Smallwood*, 113 So. 3d at 733, for cell phones are capable of storing information "wholly unlike any physical object found within a closed container." *Smith*, 920 N.E.2d at 954. Furthermore, these courts note that "[a] search of [a] cell phone's contents [is] not necessary to ensure officer safety" or to safeguard any evidence from "imminent destruction." *Id.* at 955. Consequently, these courts rely on *Chadwick* and *Gant* to hold that "warrantless cell phone data searches are *categorically* unlawful under the search-incident-to-arrest exception." *Wurie*, 2013 WL 2129119, at *10.

---

[5] While declining to base its holding on "whether there was a search incident to arrest," the Wisconsin Supreme Court also has held that police officers may not, absent exigent circumstances, conduct a warrantless search of images stored on a cell phone seized from a person they have detained and handcuffed. *State v. Carroll*, 778 N.W.2d 1, 12 & n.7 (Wis. 2010).

II. The Propriety Of Cell Phone Searches Incident To Arrest Should Be Resolved Now.

A. The Issue Greatly Affects Personal Privacy And Day-To-Day Police Operations.

1. "It is the rare arrestee today who is not found in possession of a cell phone."[6] The vast majority of American adults – approximately 91% as of June 2013 – now own a cell phone. Of those cell phone owners, 61% own smartphones, such as Apple's iPhone and the Samsung device at issue here.[7]

At the same time, police in the United States arrest thousands of people every day. In 2010 alone, there were nearly 11.5 million total adult arrests.[8] These arrests are often triggered by legal infractions as minor as failure to abide by the vehicle code. *Cf. Atwater v. City of Lago Vista*, 532 U.S. 318, 354-55 (2001) (upholding the constitutionality of the arrest of a motorist for failure to fasten her seat belt). Thus,

---

[6] M. Wesley Clark, *Searching Cell Phones Seized Incident to Arrest*, FBI L. Enforcement Bull., Feb. 2009, at 25, *available at* http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2009-pdfs/february09leb.pdf.

[7] *See* Aaron Smith, Pew Research Ctr.'s Internet & Am. Life Project, Smartphone Ownership – 2013 Update 2, *available at* http://www.pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx.

[8] Howard N. Snyder, Bureau of Justice Statistics, U.S. Dep't of Justice, Patterns and Trends: Arrest in the United States, 1990-2010, at 2 tbl.1 (2012), *available at* http://www.bjs.gov/content/pub/pdf/aus9010.pdf.

even routine arrests for minor offenses regularly give rise to the question presented. *See People v. Nottoli*, 130 Cal. Rptr. 3d 884, 893-94, 907 (Cal. Ct. App. 2011) (upholding an officer's "unqualified authority" to search data stored on an arrestee's Blackberry incident to arrest for driving under the influence).

2. In light of the frequency with which people are arrested with cell phones and the judiciary's confusion over whether the police may search the digital contents of those phones, this Court's intervention is critical. As this Court has remarked, "[w]hen a person cannot know how a court will apply a settled principle to a recurring factual situation, that person cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority." *New York v. Belton*, 453 U.S. 454, 459-60 (1981). And insofar as the courts that have spoken on the issue have reached inconsistent results, the Fourth Amendment's protections currently vary according to state and jurisdictional lines.

Such uncertainty and inconsistency should not persist. To the extent that the Fourth Amendment permits cell phone searches incident to arrest, the current confusion over the issue may cause officers to refrain, in an abundance of caution, from undertaking this investigative tactic. On the other hand, if the Fourth Amendment prohibits such searches absent exigent circumstances or a warrant, officers may be conducting searches that violate legitimate expectations of privacy. Yet all law enforcement agencies can do at the moment is lament, as one agency does in its training materials, that the law in this area is "ambiguous" and "remains

unclear."[9] As one veteran of the New York State Police force recently remarked, the "time is rapidly approaching when the Supreme Court must decide the issue and provide a comprehensive statement on the subject."[10]

B. Additional Percolation Would Not Aid This Court's Consideration Of The Issue.

There is no good reason to delay resolution of the question presented in the hopes that additional lower court opinions will unearth new legal theories or converge on a uniform legal regime.

1. The issue has now been thoroughly ventilated. Numerous federal appellate and state supreme court decisions have explored the legal arguments arising from searching cell phones seized during arrests. Indeed, at least nine such decisions have already been issued – most with dissenting opinions – and

---

[9] Mass. Mun. Police Training, Legal Update: Searching Cell Phones Incident to Arrest 2 (2012), *available at* http://www.mass.gov/eopss/docs/mptc/cell-phone.pdf; *see also* Clark, *supra*, at 26-30 (FBI bulletin noting this "uncertainty"); Computer Crime & Intellectual Prop. Section, Criminal Div., U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 32-33 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (noting that courts have "disagreed" about whether searching a cell phone incident to arrest is permissible).

[10] Terrence P. Dwyer, *Cell Phones, Privacy, and the Fourth Amendment*, PoliceOne.com (Aug. 10, 2012), http://www.policeone.com/investigations/articles/5907286-Cell-phones-privacy-and-the-Fourth-Amendment/.

some dedicating dozens of pages to the issue. *See supra* Part I.B. (By comparison, when the Solicitor General recommended, and this Court granted, certiorari in *United States v. Jones*, 132 S. Ct. 945 (2012), involving the propriety of warrantless GPS tracking, there were only four such opinions on the issue. *See* Pet. for Writ of Cert. at 20-23, *Jones*, 132 S. Ct. 945 (No. 10-1259).) These courts now openly acknowledge the increasing division. *See, e.g.*, *United States v. Wurie*, ___ F.3d ___, 2013 WL 2129119, at *5 (1st Cir. May 17, 2013); *United States v. Flores-Lopez*, 670 F.3d 803, 805 (7th Cir. 2012); *Smallwood v. State*, 113 So. 3d 724, 733 n.5 (Fla. 2013); *People v. Diaz*, Pet. App. 47a n.17 (Cal. 2011). The First Circuit recently refused to consider the issue en banc, with two judges deeming such a rehearing pointless and calling instead for this Court to resolve the issue. *United States v. Wurie*, ___ F.3d ___, 2013 WL 3869965 (1st Cir. July 29, 2013).

In addition, there is a rich body of academic scholarship exploring the doctrinal and policy-related consequences of different legal regimes that might govern this issue. One article surveys the different approaches that a court might take without itself taking a position. *See* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. Rev. 27 (2008). Another article argues that warrantless cell phone searches incident to arrest should be categorically prohibited. *See* Charles R. Maclean, *But, Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Arrest*, 6 Fed. Cts. L. Rev. 37 (2012). Still others contend that such searches should be permitted only under certain

circumstances. *See, e.g.*, Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J. L. & Pub. Pol'y 403 (2013); Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L. Rev. 183 (2010); Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-to-Arrest Exception to the Cell Phone as "Hybrid,"* 60 Drake L. Rev. 429 (2012).[11]

2. Additional percolation is particularly unlikely to reap any benefits in light of the nature of courts' disagreement over the question presented. On one side of the split, courts believe that this Court's decisions in *Robinson* and the other cases from the 1970's constitute "binding precedent" that requires

---

[11] There also are a number of student-authored works offering perceptive analyses. *See, e.g.*, Byron Kish, Comment, *Cellphone Searches: Works Like a Computer, Protected Like a Pager?*, 60 Cath. U. L. Rev. 445 (2011); Jana L. Knott, Note, *Is There an App for That? Reexamining the Doctrine of Search Incident to Arrest in the Context of Cell Phones*, 35 Okla. City U. L. Rev. 445 (2010); Ben E. Stewart, Note, *Cell Phone Searches Incident to Arrest: A New Standard Based on* Arizona v. Gant, 99 Ky. L.J. 579 (2010-2011); Chelsea Oxton, Note, *The Search Incident to Arrest Exception Plays Catch Up: Why Police May No Longer Search Cell Phones Incident to Arrest Without a Warrant*, 43 Creighton L. Rev. 1157 (2010); Leanne Anderson, People v. Diaz*: Warrantless Searches of Cellular Phones, Stretching the Search Incident to Arrest Exception Beyond the Breaking Point*, 39 W. St. U. L. Rev. 33 (2011); Ashley B. Snyder, Comment, *The Fourth Amendment and Warrantless Cell Phone Searches: When Is Your Cell Phone Protected?*, 46 Wake Forest L. Rev. 155 (2011); J. Patrick Warfield, Note, *Putting a Square Peg in a Round Hole: The Search-Incident-to-Arrest Exception and Cellular Phones*, 34 Am. J. Trial Advoc. 165 (2010).

treating searches of cell phones identically to searches of any other objects. *Diaz*, Pet. App. 47a; *see also id.* at 51a (Kennard, J., concurring) (agreeing with the majority's approval of unrestricted cell phone searches "[u]nder the compulsion of directly applicable Supreme Court precedent"); *United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007) (treating *Robinson* as controlling); *Flores-Lopez*, 670 F.3d at 805 (characterizing *Finley* and *Murphy* as relying on a "literal reading" of *Robinson*). Accordingly, these courts opine that "[i]f . . . the wisdom of [this Court's] decisions 'must be newly evaluated' in light of modern technology, then that reevaluation must be undertaken by the high court itself." *Diaz*, Pet. App. 47a (citation omitted).

On the other side of the split, courts do not think that this Court's prior cases control the outcome here. These courts perceive the digital contents of cell phones as being qualitatively different than the simple, physical items that this Court has previously treated as automatically searchable. *Smallwood*, 113 So. 3d at 731-32. That being so, these courts maintain that "*Robinson* is neither factually nor legally on point," *id.* at 730, and that it is perfectly "compatible" with this Court's jurisprudence to forbid the police from searching cell phones under the search-incident-to-arrest doctrine, *Wurie*, 2013 WL 2129119, at *10.

Only this Court can decide which of these two conflicting views of its precedent is correct.

III. This Case Is An Excellent Vehicle For The Court To Resolve The Conflict.

The facts of this case, unlike many of the others involving searches of cell phones seized during

arrests, would allow this Court to consider different variations on the propriety of cell phone searches and thus to deliver comprehensive guidance on the issue. This is so for two reasons.

First, this case involves a range of different types of digital content stored on cell phones. The officers in this case examined not only simple text viewable on rudimentary of cell phones but also photos and video recordings more characteristic of smartphones. This case thus affords this Court the opportunity to consider – as one court has suggested might be important, *see Flores-Lopez*, 670 F.3d at 809-10 – whether any particular kinds of digital content present different privacy concerns than others.

Second, petitioner challenges the constitutionality of two distinct searches of his cell phone's digital contents: one at the scene of his arrest and another at the stationhouse several hours later by an officer who was not even present at the scene during the arrest. Many cases present one or the other scenario, but rarely does a case cleanly present both.

This Court's precedent suggests that such temporal and geographic considerations could be relevant to the propriety of searching cell phones seized during arrest. In *United States v. Edwards*, 415 U.S. 800 (1974), this Court upheld a warrantless search of a detainee's clothes that he was still wearing ten hours after his arrest, stating at one point that a "reasonable delay" in effectuating a search incident to arrest does not undermine its legitimacy. *Id.* at 805. On the other hand, this Court has stated that "a search can be incident to arrest only if it is substantially contemporaneous with the arrest," *Stoner v. California*, 376 U.S. 483, 486

(1964), and that a warrantless search incident to arrest must be grounded in the "inherent necessities of the situation *at the time of the arrest*," *Chimel v. California*, 395 U.S. 752, 759 (1969) (emphasis added) (quoting *Trupiano v. United States*, 334 U.S. 699, 705, 708 (1948)). Moreover, this Court explained in *United States v. Chadwick*, 433 U.S. 1 (1977), that "warrantless searches of luggage or other property seized at the time of an arrest cannot be justified as incident to that arrest if the search is *remote in time or place* from the arrest." *Id.* at 15 (emphasis added) (internal quotation marks and citation omitted). Accordingly, if this Court were to address only a single cell phone search at the scene or later in a stationhouse, it might leave police and lower courts still unsure of the law governing the other situation.

IV. The Fourth Amendment Prohibits Searching The Digital Contents Of A Cell Phone Incident To Arrest.

Contrary to the California Supreme Court's view, the Fourth Amendment forbids police officers from searching cell phones incident to arrest for two reasons. First, once a cell phone is securely in police control, neither of the reasons identified in *Chimel v. California*, 395 U.S. 752 (1969), for conducting searches incident to arrest justifies searching the phone's digital contents. Second, the profound privacy concerns attendant to cell phones make it unreasonable for police officers to search digital content without a warrant.

A. Neither Of The *Chimel* Rationales For Searches Incident To Arrest Is Present Here.

1. As this Court has repeatedly explained, the search-incident-to-arrest exception requires a search to be "'reasonably limited' by the 'need to seize weapons' and 'to prevent the destruction of evidence.'" *Chimel*, 395 U.S. at 764 (quoting *Sibron v. New York*, 392 U.S. 40, 67 (1968)). "If there is no possibility" that the arrestee could gain access to a weapon or destroy evidence, "both justifications for the search-incident-to-arrest exception are absent and the rule does not apply." *Arizona v. Gant*, 556 U.S. 332, 339 (2009); *see also Thornton v. United States*, 541 U.S. 615, 627 (2004) (Scalia, J., concurring in the judgment) ("[C]onducting a *Chimel* search is not the Government's right; it is an exception – justified by necessity. . . .").

Neither of the *Chimel* justifications applies to the digital contents of cell phones. While officers may inspect a cell phone's physical components to detect weapons, a phone's *digital* contents – such as text messages, emails, photos, or videos – can never threaten officer safety. Furthermore, once officers separate an arrestee from his phone, they can eliminate any risk that he might destroy digital evidence on the phone. While some courts have speculated that the data in cell phones might be subject to remote "wiping" or destruction, *e.g.*, *United States v. Flores-Lopez*, 670 F.3d 803, 807-09 (7th Cir. 2012), the First Circuit has correctly recognized that officers have at least three options to prevent such action. They may turn off the phone (or put it in airplane mode); place it in an inexpensive bag that

prevents any signals from entering or escaping; or "mirror (copy) the entire cell phone contents . . . without looking at the copy." *United States v. Wurie*, ___ F.3d ___, 2013 WL 2129119, at *9 (1st Cir. May 17, 2013) (citation and internal quotation marks omitted). Thus, once a cell phone is in police custody, "the state has satisfied its immediate interest in collecting and preserving evidence." *State v. Smith*, 920 N.E.2d 949, 955 (Ohio 2009). If it wishes to search the phone's contents, it may seek a warrant. *Id.*; *cf. Missouri v. McNeely*, 133 S. Ct. 1552, 1562 (2013) (noting that police can now can obtain warrants within minutes).

2. The California Supreme Court resisted this analysis on the ground that this Court's holding in *United States v. Robinson*, 414 U.S. 218 (1973), forecloses it. According to the California Supreme Court, this Court's analysis in that case (and in subsequent cases referencing *Robinson*) affords "no legal basis" for distinguishing between a seized item itself and its contents. *People v. Diaz*, Pet. App. 25a, 43a (Cal. 2011). Once the police seize an item incident to an arrest, they automatically may "*open and examine*" the item – even digital contents within a cell phone. *Id.* 42a.

This reasoning overreads this Court's cases. *Robinson* and other cases discussing its holding stand only for the proposition that, where there is *some chance* that a search is needed to protect police or preserve evidence, courts are not required to engage in a "case-by-case adjudication" to determine "the probability in a particular arrest" that the arrestee in fact has weapons or destructible evidence. *Robinson*, 414 U.S. at 235. Thus, even though it is unlikely that

a cigarette package (or a wallet or purse) might hold a weapon, it is possible it might contain, for instance, a razor blade. Where, however, there is *no chance* that the search is necessary to discover weapons or to preserve evidence, this Court's holdings in *United States v. Chadwick*, 433 U.S. 1, 15 (1977), and *Gant* instruct that the Fourth Amendment prohibits a warrantless search. *See Chadwick*, 433 U.S. at 15 (prohibiting search of a footlocker seized during arrest); *Gant*, 556 U.S. at 343 (same for search of a vehicle incident to arrest).

The California Supreme Court pushed *Chadwick* and *Gant* aside, asserting that they are irrelevant because they "involved a search of the area within an arrestee's immediate control, not of the arrestee's person." Pet. App. 37a n.9; *see also* Pet. App. 32a-33a. Yet – as even another court on California's side of the conflict at issue has recognized – there is no basis in law or logic for distinguishing between the two situations. *See United States v. Curtis*, 635 F.3d 704, 712 (5th Cir. 2011). As this Court explained in *Chimel*, the justification necessary for a search incident to arrest is always the same, regardless of whether the police wish to search an arrestee's person or the area "within his immediate control." 395 U.S. at 762-63. In either case, the search must be justified – at least within the realm of possibility – by the need "to remove any weapons," and "to prevent [evidence] concealment or destruction." *Id.* Once "there is no longer any danger that the arrestee might gain access to [property confiscated incident to arrest] to seize a weapon or destroy evidence," the police may not search the property without obtaining a warrant. *Chadwick*, 433 U.S. at 15.

The California Supreme Court's distinction between property seized from the arrestee's "person" and property seized from his "immediate control" would also lead to arbitrary results. Under such a rule, the police could search the digital contents of any cell phone taken from someone's hands or pockets. But if the police arrested someone in her office, they apparently would be unable to search her phone if at that moment it were sitting on her desk. Or if police arrested the driver of a car, they would be unable to search a phone resting in a cupholder. Governmental access to the most sensitive details of a person's private life should hinge on more than such happenstance.

B. The Profound Privacy Concerns Related To Cell Phones Make It Unreasonable To Search Them Without Warrants.

It is also inappropriate to extend *Robinson* to cell phones because "the electronic devices that operate as cell phones of today are materially distinguishable from the static, limited-capacity" containers of the past. *Smallwood v. State*, 113 So. 3d 724, 732 (Fla. 2013). Unlike those containers, cell phones contain "vast" amounts of "very personal" information – from text-based messages to email (some of which may be confidential business material or privileged work product) to appointment records to photos and videos. *Id.* at 732-33. Indeed, a cell phone is not really even "a 'container' in any normal sense of that word." *Flores-Lopez*, 670 F.3d at 806. It is a mini, yet powerful, computer that happens to include a phone.

A cell phone, therefore, should not be treated as "a closed container for purposes of a Fourth

Amendment analysis." *Smith*, 920 N.E.2d at 954. To hold otherwise – and thus to "allow[] the police to search [the data on a cell phone] without a warrant any time they conduct a lawful arrest" – would "create 'a serious and recurring threat to the privacy of countless individuals.'" *Wurie*, 2013 WL 2129119, at *12 (quoting *Gant*, 556 U.S. at 345); *see also* Elizabeth Woyke, *Debate Over Warrantless Cellphone Searches Heats Up*, Forbes (Sept. 7, 2011), http://www.forbes.com/sites/elizabethwoyke/2011/09/07/debate-over-warrantless-cellphone-searches-heats-up/ (explaining that allowing such searches would expose sensitive information commonly stored on businesspersons' cell phones to governmental view).

The California Supreme Court deemed the distinction between cell phones and ordinary containers immaterial, asserting that this Court's decisions "do not support the view that whether the police must get a warrant before searching an item they have properly seized from an arrestee's person incident to a lawful custodial arrest depends on the item's character, including its capacity for storing personal information." Pet. App. 35a (emphasis omitted). In particular, the California Supreme Court asserted that *New York v. Belton*, 453 U.S. 454 (1981), and *United States v. Ross*, 456 U.S. 798 (1982), "expressly rejected the view that the validity of a warrantless search depends on the character of the searched item." *Diaz*, Pet. App. 36a-37a.

But neither case controls here. As the First Circuit has noted, this Court, "more than thirty-five years ago, could not have envisioned a world in which the vast majority of arrestees would be carrying on their person an item containing not physical evidence

but a vast store of intangible data – data that is not immediately destructible and poses no threat to the arresting officers." *Wurie*, 2013 WL 2129119, at *10. Indeed, this Court in *Belton* characterized a "container" as "any object capable of holding another object." 453 U.S. at 460 n.4. This description bespeaks something that holds physical items, not mere digital text and images.

It bears remembering, moreover, that "the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995). "[T]he reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

Applying this traditional default formula to the situation here yields a clear outcome: searching a cell phone without a warrant intrudes on personal privacy to an extraordinary degree, and is unnecessary to serve any legitimate governmental interest this Court has identified in its search-incident-to-arrest cases. Indeed, several current Members of this Court have recognized in the related context of GPS tracking that the Fourth Amendment must be sensitive to new technologies enabling police to easily obtain massive amounts of personal information that, at least as a practical matter, would previously have been inaccessible. *See United States v. Jones*, 132 S. Ct. 945, 955-56 (2012)

(Sotomayor, J., concurring); *id.* at 963-64 (Alito, J., concurring in the judgment). Cell phones have wrought just this kind of technological sea change. Accordingly, the Fourth Amendment should require the detached scrutiny of a neutral magistrate before allowing the police to rummage through the digital contents of such a device. Anything less would unduly safeguard the intimate details of the citizenry's business dealings and private affairs.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Patrick Morgan Ford
ATTORNEY AT LAW
1901 First Avenue
Suite 400
San Diego, CA 92101

Kevin K. Russell
GOLDSTEIN &
RUSSELL, P.C.
5225 Wisconsin Ave., NW
Suite 404
Washington, DC 20036

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

July 30, 2013

APPENDIX

APPENDIX A

COURT OF APPEAL

Fourth District, Division 1, California

The PEOPLE, Plaintiff and Respondent,

v.

David Leon RILEY, Defendant and Appellant.

D059840 | Filed February 8, 2013

APPEAL from a judgment of the Superior Court of San Diego County, Laura W. Halgren, Judge. Affirmed. (Super. Ct. No. SCD226240)

McDONALD, J.

A jury convicted defendant David Riley of one count of shooting at an occupied vehicle (Pen. Code, § 246,[1] count 1), one count of attempted murder (§§ 664/187, subd. (a), count 2) and one count of assault with a semi-automatic firearm (§ 245, subd. (b), count 3), and found true numerous enhancements appended to counts 1 through 3.[2] The court sentenced Riley to 15 years to life.

On appeal, Riley contends (1) the court erred when it denied his motions to suppress evidence obtained in the search of his vehicle and the later search of his cell

---

[1] All further statutory references are to the Penal Code unless otherwise specified.

[2] The jury found two firearm enhancements (under § 12022.53, subds. (b) & (e)(1)) in connection with count 2 to be true, and found true that he personally used a firearm within the meaning of section 12022.5, subdivision (a), in connection with count 3, and found true the allegation (as to each count) that he committed the offenses for the benefit of a criminal street gang within the meaning of section 186.22, subdivision (b).

phone; (2) the prosecution of the current offenses violated the *Kellett*[3] rule, and (3) the prosecutor engaged in prejudicial misconduct when questioning a witness.

I.

FACTS

A. *Prosecution Evidence*

The Shooting

Riley belonged to the Lincoln Park gang. Around 2:30 p.m. on August 2, 2009, an Oldsmobile belonging to Riley was parked in front of the Urias family home near an intersection in the Skyline neighborhood of San Diego. Riley's girlfriend, Jazmin McKinnie (who lived down the street from the Uriases' house), was standing and talking with three men near Riley's car.

Mr. Webster, a member of a rival gang, drove his car through the intersection. The three men standing near Riley's car fired numerous shots at Webster's car. Webster's car crashed into something. The shooters got into Riley's Oldsmobile and drove away. Numerous shell casings from at least two different guns (a .40 caliber handgun and a .45 caliber handgun) were found at the scene. Police found Riley's Oldsmobile the next day in a Lincoln Park gang area. It was almost completely hidden under a car cover. The three eyewitnesses to the shooting declined to give a positive identification of Riley as one of the shooters, although one of those witnesses said Riley could have been one of the shooters.[4]

---

[3] *Kellett v. Superior Court* (1996) 63 Cal. 2d 822 (*Kellett*).

[4] Mr. Haddock was identified as being involved based on a positive identification from an eyewitness, and another man

The Stop and Search

On August 22, 2009, Riley was driving his other car (a Lexus) when he was stopped by police. A search of the car found a .40 caliber handgun and a .45 caliber handgun hidden in a sock inside the engine compartment.[5] Ballistics testing confirmed these two weapons were used in shooting at Webster's car. DNA testing confirmed Riley and two other men were possible contributors for the samples taken from one of the handguns, and Haynes and two other men were possible contributors to the sample taken from the other handgun.

Riley was arrested as a result of this stop and police seized his cell phone. Cell phone records showed Riley's phone was used near the place of the shooting at around the time of the shooting, and was used about 30 minutes later near the location where police found Riley's Oldsmobile. The cell phone contained pictures of Riley making gang signs.

Riley's Jailhouse Statements

While in jail, Riley made several phone calls that were recorded and played to the jury. In an August 24, 2009, phone call, Riley asked the other person (an unidentified female) about "what exactly did my charges say?" When she responded there were "gun charges," he asked, "But did it have – did it have any shooting stuff? It just had gun charges[,] right?" When she told Riley it was limited to gun charges and driving without a license, he asked, "No type of

---

belonging to Riley's gang (Mr. Haynes) was tied to the shooting by DNA evidence found on the gun used in the shooting.

[5] The facts surrounding the stop and search are more fully discussed below.

shooting or any . . ." and she replied, "it had some other stuff. I don't know what it means though," and Riley stated, "it would say like attempted something or something like that." In another phone call two days later, he mentioned "like no way that that shit is, it's gonna come back to me like no matter what, the ballistics, it's gonna show. . . ." In another call that day, he told McKinnie his "main focus" was getting bailed out and "[t]he reason why I'm trying to get bailed out is because I know what they got and I know what's [going to] hit eventually." During that same call, after telling her he was "trying to hit third world countries . . . [bec]ause I'm trying to get, really," Riley stated, "I'm waiting for these . . . mother fuckin' whoopties [6] to come back . . . and it's a rap, so before then, I'm trying to be 5000, 50, 50 world states up out [of] this mother fucker though."

Gang Evidence

A gang expert testified to Riley's membership in the Lincoln Park gang, the rivalry between Riley's gang and the gang to which the shooting victim belonged, and why the shooting could have been motivated to further the Lincoln Park gang.

II.

ANALYSIS OF RILEY'S SEARCH AND SEIZURE CLAIM

Riley contends the trial court erred when it denied his motions to suppress the evidence obtained in the search of his car, which yielded the handgun, and the search of his cell phone, which yielded videos and photographs showing Riley's gang affiliation.

---

[6] McKinnie testified a "whooptiwopper" or "whooptiwham" is slang that can mean a gun.

A. *Relevant Facts from the Suppression Hearing*

The Stop and Impound Decision

About three weeks after the shooting, San Diego Police Officer Dunnigan stopped Riley because the registration tags on Riley's Lexus had expired. After learning Riley was driving with a suspended driver's license, Dunnigan asked him to get out of the car because he intended to impound it. Just before Riley got out of the car, he started to reach into his pocket and Dunnigan warned Riley not to do so. Riley replied he was reaching for his cell phone. Dunnigan decided to impound Riley's car because, with few exceptions, the policy of the police department is to impound and tow a vehicle when the driver who is stopped is driving without a valid license, because police want to ensure the person with the suspended license cannot return to the car and drive away.

Discovery of the Guns

Dunnigan testified that, when an officer decides to impound a vehicle, departmental policy requires that police conduct an inventory search of the vehicle. The primary reason for an impound inventory search is to limit the City's liability by protecting against claims that items in the car at the time of the impound were missing when the car is returned to the owner. The list of items on the impound slip includes items under the hood of the car, including the battery and the alternator, that are to be inventoried.

Dunnigan was standing on the curb with Riley, issuing the citation for driving with a suspended license, when Officer Ruggerio arrived to assist Dunnigan with the stop and the impound and

inventory search. Ruggerio conducted the inventory search, which included looking under the hood. He normally checks under the hood because the impound sheet requires the officer to check off that none of the pieces are missing, and because he has found contraband under the hood on prior occasions. When Ruggerio found the guns under the hood, he showed the guns to Dunnigan, who decided to place Riley under arrest.

At the time of the stop, impound and inventory search, Dunnigan did not know who Riley was or anything about the shooting incident. The decision to stop the car was based on the registration violation, and the decision to impound the car (and the concomitant inventory search) was motivated by Dunnigan's adherence to departmental policy after he learned of Riley's invalid driver's license.

The Cell Phone

After finding the guns and some other gang paraphernalia, and placing Riley under arrest based on the guns, Dunnigan contacted Detective Malinowski, a detective specializing in gangs. Dunnigan contacted Malinowski because of the presence of the loaded guns and because Dunnigan saw several indicia of gang affiliation. One of those indicia was that, when Dunnigan looked at Riley's cell phone, he noticed all of the entries starting with the letter "K" were preceded by the letter "C," which gang members use to signify "Crip Killer."

Detective Malinowski went to the police station in response to Dunnigan's call. At the station, the arresting officers gave the cell phone to Malinowski when he asked for any property found on Riley.

Malinowski looked through the phone and found some video clips of young men street boxing and heard Riley's voice in the background encouraging the fighters. He also found some photographs.

The Ruling

The trial court first evaluated the motion to suppress the guns. It found credible the testimonies of Dunnigan and Ruggerio that they did not know Riley when Dunnigan stopped him, and the officers did not know anything about the shooting investigation or that Malinowski was looking for guns. The trial court also found credible that neither the initial stop (based on the expired registration) nor the decision to impound the car (when Dunnigan learned of the invalid driver's license) were pretextual, and the decision to impound was based on Dunnigan's ordinary practice rather than being motivated by an improper investigatory purpose. It also found the officers were following the police department procedures when they conducted the inventory search, which includes a checklist that specifies looking under the hood, and there were legitimate reasons (including protecting the department against later claims of liability) underlying that general procedure. Accordingly, the court denied the motion to suppress the fruits of the inventory search.

The court reserved ruling on the issue of the cell phone search to consider additional legal authorities. After reading additional authorities, the court stated "the cell phone, which as I understand it was on [Riley's] person at the time of the arrest, would fall into the category of a booking search, the scope of which is very broad," and was therefore inclined to uphold the search. The trial court offered the parties

the opportunity to "see if there's anything else you want me to consider" before it ruled on the cell phone search, and stated it would wait a few days to issue its ruling. When court resumed, it ruled the search of the cell phone was lawful, concluding the reasoning in *People v. Diaz* (review granted October 28, 2008, S166600), an appellate decision then on review before the California Supreme Court and subsequently affirmed and superseded by *People v. Diaz* (2011) 51 Cal. 4th 84 (*Diaz*), made sense and would permit a search of the cell phone found on Riley's person when he was arrested.

B. ***Applicable Law***

Inventory Searches

The Fourth Amendment to the United States Constitution protects people from unreasonable government intrusions into their legitimate expectations of privacy and, when a warrantless search is involved, the burden is on the prosecution to justify the search by proving the search fell within a recognized exception to the warrant requirement. (*In re Tyrell J.* (1994) 8 Cal. 4th 68, 76, disapproved on other grounds by *In re Jaime P.* (2006) 40 Cal. 4th 128, 139.)

"[A] law enforcement officer may, consistent with the Fourth Amendment, briefly detain a vehicle if the objective facts indicate that the vehicle has violated a traffic law. The officer's subjective motivation in effecting the stop is irrelevant." (*People v. White* (2001) 93 Cal. App. 4th 1022, 1025.) If the officer determines, during an otherwise lawful stop, that the driver is driving on a suspended license, the officer has justification to impound that vehicle. (*People v.*

Duncan (2008) 160 Cal. App. 4th 1014, 1019; *People v. Benites* (1992) 9 Cal. App. 4th 309, 326 [impoundment proper where neither driver nor passenger had valid driver's license]; *People v. Burch* (1986) 188 Cal. App. 3d 172 [impoundment proper where car's registration tag was expired and driver's license was suspended]; *South Dakota v. Opperman* (1976) 428 U.S. 364, 368-369 (*Opperman*) [as part of their "'community caretaking functions,'" police officers may constitutionally impound vehicles that "jeopardize . . . public safety and the efficient movement of vehicular traffic"].)

When an officer is warranted in impounding a vehicle, a warrantless inventory search of the vehicle pursuant to a standardized procedure is constitutionally reasonable. (*Opperman, supra,* 428 U.S. at pp. 371-372.) When an inventory search is conducted based on a decision to impound a vehicle, we "focus on the purpose of the impound rather than the purpose of the inventory," because an inventory search conducted pursuant to an unreasonable impound is itself unreasonable. (*People v. Aguilar* (1991) 228 Cal. App. 3d 1049, 1053.) The language in several United States Supreme Court decisions has suggested that, when considering the validity of an inventory search, the officer's motive for the decision to impound the vehicle can invalidate the inventory search if the decision to impound was subjectively motivated by an improper investigatory purpose. (*See, e.g., Opperman,* at p. 376; *Colorado v. Bertine* (1987) 479 U.S. 367, 372, 376.) Accordingly, California courts have concluded that "[t]he relevant question is whether the impounding was subjectively motivated by an improper investigatory purpose." (*People v. Torres* (2010) 188 Cal. App. 4th 775, 791 (*Torres*).)

Searches of Property Taken from the Defendant's Person Incident to Arrest

The California Supreme Court has recently confirmed that a delayed search of an item immediately associated with the arrestee's person may be justified as incident to a lawful custodial arrest without consideration as to whether an exigency for the search exists. (*Diaz, supra,* 51 Cal. 4th 84.) In *Diaz,* as here, police conducted a postarrest search of a cell phone found on the defendant's person. (*Id.* at p. 89.) On appeal from the denial of his motion to suppress, the defendant argued the search of his cell phone "'was too remote in time' to qualify as a valid search incident to his arrest. In making this argument, he emphasize[d] that the phone 'was exclusively held in police custody well before the search of its text message folder.'" (*Id.* at p. 91, fn. omitted.) In rejecting this argument, the *Diaz* court focused on one key question: "whether defendant's cell phone was 'personal property . . . immediately associated with [his] person' [citation] . . . ." (*Id.* at p. 93.) As the court explained, "[i]f it was, then the delayed warrantless search was a valid search incident to defendant's lawful custodial arrest. If it was not, then the search, because it was '"remote in time [and] place from the arrest,"' 'cannot be justified as incident to that arrest' unless an 'exigency exist[ed].'" (*Id.* at p. 93, fn. omitted.) Ultimately, the *Diaz* court held the cell phone was immediately associated with the defendant's person and, therefore, the warrantless search of the cell phone was valid, stating that "[b]ecause the cell phone was immediately associated with defendant's person, [the officer] was 'entitled to inspect' its contents without a warrant [citation] at the sheriff's station 90 minutes after defendant's arrest,

whether or not an exigency existed." (*Id.* at p. 93, fn. omitted.)

Standard of Review

In ruling on a motion to suppress, the trial court judges the credibility of the witnesses, resolves any conflicts in the testimony, weighs the evidence, and draws factual inferences. We will uphold the court's express and/or implied findings on such matters if they are supported by substantial evidence, but we independently review the application of the relevant law to the facts. (*People v. Alvarez* (1996) 14 Cal. 4th 155, 182.)

C. *Analysis*

The Inventory Search

There is substantial evidence to support the conclusion that both the initial stop and the subsequent decision to impound the car were based on legitimate motives rather than as a ruse to conduct an investigatory search. Dunnigan testified, and the trial court found credible, that he did not know Riley (and was unaware Riley might have been involved in the shootings) when he decided to impound the vehicle, and that his decision to impound was based on the fact Riley did not have a valid driver's license and was consistent with Dunnigan's ordinary practice. There was also substantial evidence that the scope of the inventory search was based on legitimate reasons rather than being motivated by an improper investigatory purpose: the officers were following police department procedures when they conducted the inventory search, which includes a checklist that specifies looking under the hood to assess what was present under the hood, and there was evidence that

legitimate reasons (e.g., protecting the department against later claims of liability when the impounded vehicle is returned to the owner) underlay that general procedure.

The cases cited by Riley do not undermine our conclusion. In *People v. Williams* (2006) 145 Cal. App. 4th 756, a driver was stopped and presented a valid driver's license; however, the driver could not present a registration or proof of insurance for the car, which was validly registered to a car rental company and had not been reported stolen. The officer arrested the defendant based on an outstanding warrant and impounded the car. The court concluded the impound was invalid because, after noting the police department had no written policy addressing when a car should be impounded and such decision was left entirely to each officer's discretion, it reasoned:

> The prosecution, which had the burden of establishing that impounding appellant's car was constitutionally reasonable under the circumstances, *made no showing that removal of the car from the street furthered a community caretaking function*. Morton admitted that the car was legally parked in front of appellant's residence, appellant had a valid driver's license, the car was properly registered to a car rental company, the car had not been reported stolen, and he had no reason to believe appellant was not in lawful possession of the car. [¶] . . . [¶] No community caretaking function was served by impounding appellant's car. The car was legally parked at the curb in front of appellant's home. . . . *Because appellant had a valid driver's license and the car was properly registered, it was not*

> *necessary to impound it to prevent immediate and continued unlawful operation.*

(*Id.* at pp. 762-763, italics added.)

In contrast, the prosecution here *did* satisfy its burden of establishing that impounding appellant's car was constitutionally reasonable under the circumstances by showing removal of the car from the street furthered a community caretaking function: Riley did not have a valid license, and the car did not have a valid registration. Impounding was necessary to prevent the immediate and continued unlawful operation of the car.

The decision in *Torres*, *supra*, 188 Cal. App. 4th 775 is even less apposite. In *Torres*, the deputy pulled the defendant over for an unsafe lane change and failure to signal a turn. The defendant driver parked in a stall in a public parking lot and got out of the truck, and told the officer he did not have a valid driver's license. The deputy decided to impound the truck. (*Id.* at p. 780.) The defendant contended the search was a prohibited, "pretextual" inventory search because the deputy conceded at the suppression hearing that narcotics officers had asked him to manufacture a reason to detain and search the truck, and the deputy agreed he decided to impound the truck "'to facilitate an inventory search' to look 'for whatever narcotics-related evidence might be in the [truck].'" (*Id.* at p. 786.) The court concluded the impound and inventory search were unreasonable, noting:

> The relevant issue is the deputy's motive for impounding the truck – did he impound the truck to serve a community caretaking function

> or as a pretext for conducting an investigatory search? The record on that motion – namely, the preliminary hearing transcript – shows an investigatory motive. The deputy testified he decided to impound the truck "in order to facilitate an inventory search" because narcotics officers had asked him to "develop some basis for stopping" defendant. The deputy agreed he "basically us[ed] the inventory search as the means to go look for whatever narcotics-related evidence might be in the [truck]." (*Cf. Opperman, supra*, 428 U.S. at p. 376 [inventory search may not be "a pretext concealing an investigatory police motive"]; *Bertine, supra*, 479 U.S. at p. 376 [inventory search improper when police officers impound vehicle "in order to investigate suspected criminal activity"].) [¶] . . . The deputy did not claim defendant's lack of a license was the sole motivation for the impounding. [Citation.] . . . And he did not offer any community caretaking function served by impounding defendant's truck. The prosecution failed to show the truck was illegally parked, at an enhanced risk of vandalism, impeding traffic or pedestrians, or could not be driven away by someone other than defendant.

(*Torres, supra*, 188 Cal. App. 4th at pp. 789-790).

In contrast, the officer here testified he did not even know who Riley was when he stopped him. Moreover, the officer explained he was motivated to impound the car because Riley did not have a valid license, not because the officer was instructed to develop a basis to conduct an inventory search, and the unregistered status of the vehicle precluded

someone other than the defendant from simply driving it away. *Torres* has no application here.

The Cell Phone Search

Diaz controls the present case, and the key question is whether Riley's cell phone was "immediately associated" with his "person" when he was stopped. (*Diaz, supra*, 51 Cal. 4th at p. 93.) Relying on the evidence introduced at the suppression hearing, the trial court found "the cell phone, which as I understand it was on [Riley's] person at the time of the arrest, would fall into the category of a booking search, the scope of which is very broad," and on this basis upheld the search. This finding, supported by the evidence, establishes that Riley's cell phone was immediately associated with his person when he was arrested, and therefore the search of the cell phone was lawful whether or not an exigency still existed. (*Diaz, supra,* 51 Cal. 4th at p. 93.)

Riley argues *Diaz* is not controlling because there was some evidence, subsequently introduced at trial, showing he had taken the cell phone from his pocket and placed it on the seat of the car, and therefore the phone was not "immediately associated" with his "person" when he was arrested. However, the People correctly point out that an appellate challenge to a ruling on a pretrial evidentiary motion to suppress and exclude evidence "must be reviewed on the record as it existed when the court decided the motion" (*Torres, supra*, 188 Cal. App. 4th at p. 780; cf. *People v. Welch* (1999) 20 Cal. 4th 701, 739), not on evidence later introduced at trial.

III

THE "*KELLETT*" CLAIM

Riley argues the current prosecution is barred by the *Kellett* rule.

A. *Background*

In the first filed case (the weapons case), Riley was charged with carrying concealed firearms in a vehicle (former Pen. Code, § 12025, subd. (a)(1)) and carrying loaded firearms in a public place (former Pen. Code, § 12031, subd. (a)(1)). The weapons case was apparently filed based on the guns found during the August 22, 2009, stop and search of his vehicle. Riley pleaded guilty to those charges on October 8, 2009. The probation and sentencing hearing on those convictions was trailed to the present case, and he was ultimately sentenced on the weapons case at the same hearing sentence was imposed in the present case.

In the present case, filed approximately five months after he entered his guilty plea – but before sentencing – in the weapons case, Riley was charged with (among other things) shooting at an occupied vehicle, attempted murder, and assault with a semi-automatic firearm. Riley subsequently filed a motion in the present case arguing prosecution was barred under the *Kellett* rule. His motion asserted the prosecution was, or should have been, aware that all of the offenses charged in the weapons case and the present case were ones in which the same act or course of conduct played a significant part, within the meaning of section 654, which barred the second prosecution. The prosecution's written opposition argued *Kellett* applies only when the offenses arise out of the same act, incident, or course of conduct within

the meaning of section 654, but does not apply when the acts are distinct, and the charges in the weapons case involved criminal conduct distinct from that underlying the charges in the present case. The prosecution also asserted *Kellett* applies only when the prosecution knows or should have known of the separate offenses, and argued *Kellett* was therefore inapplicable because the evidence demonstrated the prosecution lacked forensic evidence tying Riley to the current offenses until after he had already pleaded guilty to the weapons case.

B. ***Applicable Law***

Section 654 prohibits both multiple punishment and multiple prosecution. In *Kellett, supra*, 63 Cal. 2d 822, the Supreme Court, construing section 654 in the context of the legislative policy of section 954, explained the different purposes of the two clauses of section 654. The prohibition against multiple punishment is designed "to ensure that a defendant's punishment will be commensurate with his culpability." (*People v. Correa* (2012) 54 Cal. 4th 331, 341.) Multiple prosecution, on the other hand, is prohibited to avoid "needless harassment and the waste of public funds . . . ." (*Kellett*, at p. 827.) The prohibition does not come into play unless "the prosecution is or should be aware of more than one offense *in which the same act or course of conduct plays a significant part* . . . ." (*Id.* at p. 827, italics added.) Under *Kellett*, if these criteria are met *and* the first proceeding "culminate[s] in either acquittal or conviction and sentence," the later prosecution can be barred. (*Id.* at p. 827.)

C. *Analysis*

We conclude Riley's *Kellett* claim must be deemed forfeited. The court in *People v. Jones* (1998) 17 Cal. 4th 279, 313 noted a claim based on *Kellett* may not be raised on appeal if not preserved at trial, an application of the general rule that a defendant may not raise on appeal an argument not pursued at trial. (*People v. Clark* (1993) 5 Cal. 4th 950, 988, fn. 13, disapproved on other grounds by *People v. Doolin* (2009) 45 Cal. 4th 390, 421, fn. 22.) This prohibition has particular force when the argument involves disputed factual issues not resolved below. (*See, e.g., People v. Zito* (1992) 8 Cal. App. 4th 736, 742.)

Although Riley did file a motion raising *Kellett*, the record contains no information that, once the prosecution filed its opposition pointing out the defects in the motion, Riley ever sought a ruling on his motion. It is not enough to merely file a motion, because a "defendant may forfeit the issue for appellate review by failing to press for a hearing or by acquiescing in the court's failure to hear the . . . motion." (*People v. Braxton* (2004) 34 Cal. 4th 798, 814; accord, *People v. Brewer* (2000) 81 Cal. App. 4th 442, 459-462.) Here, Riley's apparent abandonment of his *Kellett* motion leaves a crucial evidentiary vacuum, because there was no opportunity for the trial court to make the factual determination of whether the prosecution knew (or in the exercise of reasonable diligence should have known) there was enough evidence to prosecute Riley for the present case at the time it filed the weapons case. (*Cf. Barriga v. Superior Court* (2012) 206 Cal. App. 4th 739, 748 [whether the government exercised due diligence is a question of fact].) Indeed, in the specific context of a *Kellett* claim,

our Supreme Court in *People v. Davis* (2005) 36 Cal. 4th 510 noted there is a "recognized . . . exception to the multiple-prosecution bar where the prosecutor 'is unable to proceed on the more serious charge at the outset because the additional facts necessary to sustain that charge have not occurred or have not been discovered despite the exercise of due diligence.' [Citations.] . . . But this exception applies only when the government 'acted with due diligence at the outset but was unable to discover the additional facts necessary to sustain the greater charge.' [Citation.] Whether the government exercised due diligence is a question of fact." (*Id.* at p. 558.) We conclude that, having deprived the prosecution of the opportunity to have dispositive factual issues resolved in a manner that could have been fatal to Riley's *Kellett* motion, Riley has forfeited his *Kellett* claim.[7]

---

[7] Riley asserts that we should nevertheless reach the issue to forestall a claim of ineffective assistance of counsel. However, that claim requires, among other things, a showing there was "a reasonable probability that defendant would have obtained a more favorable result absent counsel's shortcomings." (*People v. Cunningham* (2001) 25 Cal. 4th 926, 1003.) We have substantial doubt Riley can satisfy that showing, because the prosecution presented significant reasons for why it neither knew nor should have known of the present case at the time it filed the weapons case. More importantly, *Kellett*'s bar applies only when "the initial proceedings culminate in either acquittal or *conviction and sentence*." (*Kellett, supra,* 63 Cal. 2d at p. 827, italics added.) Here, the probation and sentencing hearing on the convictions in the weapons case was trailed to the present case, and he was ultimately sentenced on the weapons case at the same hearing sentence was imposed on the present case. Under those circumstances, it appears *Kellett* would *not* bar the second prosecution. (*See In re R.L.* (2009) 170 Cal. App. 4th 1339, 1343-1344; *cf. People v. Andrade* (1978) 86 Cal. App. 3d 963, 971; *People v. Tideman* (1962) 57 Cal. 2d 574, 586; *People v. Hartfield*

IV

THE PROSECUTORIAL MISCONDUCT CLAIM

Riley contends an implied reference at trial to his custodial status requires reversal on appeal because it was so inflammatory it denied him a fair trial.

A. *Background*

Riley's sister was called as a defense witness to testify that Riley often loaned his Oldsmobile to friends. On cross-examination, she conceded she had not told police of this fact until sometime in early 2011, and had told the defense of this fact in December 2010. In an attempt to show this claim was a recent fabrication planted by Riley, the prosecutor asked if she had first told the defense investigator of this fact on January 21, 2011, just one day after she had met with her brother. When Riley's sister responded, "I don't remember the date I visited [Riley]," the prosecutor asked, "If I showed you the visitor['s] log, would it refresh your recollection?" The court interrupted and, after an unreported sidebar conference, the prosecutor rephrased the question to ask whether she had talked to Riley before she spoke with the investigator, and she responded "[y]es."

After testimony concluded, the court made a record of the unreported sidebar. The court stated the visitor's log referred to by the prosecutor was likely a jail log, and the court had required the prosecutor to rephrase the question because the jury had not been told Riley was in custody and steps had been taken to

---

(1970) 11 Cal. App. 3d 1073, 1080; *People v. Winchell* (1967) 248 Cal. App. 2d 580, 588.)

avoid alerting the jury to Riley's custodial status. Riley, arguing the jury could "glean" that the log referred to a jail log, moved for a mistrial. The court, noting it did not believe there was intentional conduct by the prosecutor to bring the jail issue before the jury, denied the motion for a mistrial.

B. *Legal Framework*

The applicable federal and state standards regarding prosecutorial misconduct are well established. "'A prosecutor's . . . intemperate behavior violates the federal Constitution when it comprises a pattern of conduct "so egregious that it infects the trial with such unfairness as to make the conviction a denial of due process."'" (*People v. Gionis* (1995) 9 Cal. 4th 1196, 1214.) Conduct by a prosecutor that does not render a criminal trial fundamentally unfair is prosecutorial misconduct under state law only if it involves "the use of deceptive or reprehensible methods to attempt to persuade either the court or the jury." (*People v. Espinoza* (1992) 3 Cal. 4th 806, 820.) However, to preserve a claim of misconduct on appeal, a defendant must both object and request a curative admonition (*People v. Montiel* (1993) 5 Cal. 4th 877, 914), and not doing so forfeits the claim of misconduct. (*People v. Silva* (2001) 25 Cal. 4th 345, 373.)

C. *Analysis*

Although Riley apparently objected to the reference, he did not request a curative admonition. Accordingly, the claim is forfeited. Riley argues, relying on *People v. Hill* (1998) 17 Cal. 4th 800, a defendant is excused from that requirement when a request for a curative instruction would have been futile. However, the court's observation in *People v.*

Dykes (2009) 46 Cal. 4th 731 requires that we reject Riley's argument that he was excused from the requirements of objection and request for an admonition:

> Defendant contends that his failure to object to various asserted instances of misconduct should not stand as a barrier to appellate review of his claims. He argues that an objection and admonition would have been futile, because the misconduct was pervasive and created a "hostile trial atmosphere." As our discussion has demonstrated, the prosecutor did not engage in pervasive misconduct. Defendant's reliance upon *People v. Hill, supra,* 17 Cal. 4th 800, is misplaced. Unlike that case, which we have characterized as representing an "extreme" example of pervasive and corrosive prosecutorial misconduct that persisted throughout the trial [citation], the present case did not involve counsel experiencing – as did counsel in *Hill* – a "constant barrage" of misstatements, demeaning sarcasm, and falsehoods, or ongoing hostility on the part of the trial court, to appropriate, well-founded objections.

(*Id.* at pp. 774-775.)

Here, the alleged misconduct was a single question that only briefly and indirectly alluded to the possibility Riley had been in custody several months earlier. "The isolated reference to [a defendant's custodial status] was not so grave that a curative instruction would not have mitigated any possible prejudice to defendant." (*People v. Valdez* (2004) 32 Cal.4th 73, 125.) We conclude Riley's claim of misconduct is forfeited.

DISPOSITION

The judgment is affirmed.

WE CONCUR:

NARES, Acting P.J.

McINTYRE, J.

APPENDIX B

Court of Appeal, Fourth Appellate District,

Division One – No. D059840

S209350

IN THE SUPREME COURT OF CALIFORNIA

En Banc

THE PEOPLE, Plaintiff and Respondent,

v.

DAVID LEON RILEY, Defendant and Appellant.

The petition for review is denied.

SUPREME COURT
FILED
May -1 2013
Frank A. McGuire Clerk
Deputy

CANTIL SAKAUYE
Chief Justice

APPENDIX C

Filed 1/3/11

IN THE SUPREME COURT OF CALIFORNIA

THE PEOPLE, Plaintiff and Respondent, v. GREGORY DIAZ, Defendant and Appellant.	S166600 Ct. App. 2/6 B203034 Ventura County Super. Ct. No. 2007015733

We granted review in this case to decide whether the Fourth Amendment to the United States Constitution permits law enforcement officers, approximately 90 minutes after lawfully arresting a suspect and transporting him to a detention facility, to conduct a warrantless search of the text message folder of a cell phone they take from his person after the arrest. We hold that, under the United States Supreme Court's binding precedent, such a search is valid as being incident to a lawful custodial arrest. We affirm the Court of Appeal's judgment.

FACTUAL BACKGROUND

About 2:50 p.m. on April 25, 2007, Senior Deputy Sheriff Victor Fazio of the Ventura County Sheriff's Department witnessed defendant Gregory Diaz participating in a police informant's controlled purchase of Ecstasy. Defendant drove the Ecstasy's seller to the location of the sale, which then took place in the backseat of the car defendant was driving. Immediately after the sale, Fazio, who had listened in

on the transaction through a wireless transmitter the informant was wearing, stopped the car defendant was driving and arrested defendant for being a coconspirator in the sale of drugs. Six tabs of Ecstasy were seized in connection with the arrest, and a small amount of marijuana was found in defendant's pocket. Defendant had a cell phone on his person.

Fazio transported defendant to a sheriff's station, where a detective seized the cell phone from defendant's person and gave it to Fazio. Fazio put it with the other evidence and, at 4:18 p.m., interviewed defendant. Defendant denied having knowledge of the drug transaction. After the interview, about 4:23 p.m., Fazio looked at the cell phone's text message folder and discovered a message that said "6 4 80."[1] Based on his training and experience, Fazio interpreted the message to mean "[s]ix pills of Ecstasy for $80." Within minutes of discovering the message (and less than 30 minutes after the cell phone's discovery), Fazio showed the message to defendant. Defendant then admitted participating in the sale of Ecstasy.

Defendant was charged with selling a controlled substance (Health & Saf. Code, § 11379, subd. (a)). He pleaded not guilty and moved to suppress the fruits of the cell phone search – the text message and the statements he made when confronted with it – arguing that the warrantless search of the cell phone violated the Fourth Amendment. The trial court denied the motion, explaining: "The defendant was under arrest for a felony charge involving the sale of drugs. His

---

[1] Fazio had to manipulate the phone and go to several different screens to access the text message folder. He did not recall whether the cell phone was on when he picked it up to look through it.

property was seized from him. Evidence was seized from him. [¶] . . . [I]ncident to the arrest[,] search of his person and everything that that turned up is really fair game in terms of being evidence of a crime or instrumentality of a crime or whatever the theory might be. And under these circumstances I don't believe there's authority that a warrant was required." Defendant then withdrew his not guilty plea and pleaded guilty to transportation of a controlled substance. The trial court accepted the plea, suspended imposition of sentence, and placed defendant on probation for three years.

The Court of Appeal affirmed, finding that under governing high court precedent, because the cell phone "was immediately associated with [defendant's] person at the time of his arrest," it was "properly subjected to a delayed warrantless search." We granted defendant's petition for review.

DISCUSSION

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Under this provision, as the United States Supreme Court has construed it, warrantless searches – i.e., "searches conducted outside the judicial process, without prior approval by judge or magistrate" – "are *per se* unreasonable . . . subject only to a few specifically established and well-delineated

exceptions." (*Katz v. United States* (1967) 389 U.S. 347, 357, fns. omitted.)

One of the specifically established exceptions to the Fourth Amendment's warrant requirement is "a search incident to lawful arrest." (*United States v. Robinson* (1973) 414 U.S. 218, 224 (*Robinson*).) This exception "has traditionally been justified by the reasonableness of searching for weapons, instruments of escape, and evidence of crime when a person is taken into official custody and lawfully detained. [Citation.]" (*United States v. Edwards* (1974) 415 U.S. 800, 802-803 (*Edwards*).) As the high court has explained: "When a custodial arrest is made, there is always some danger that the person arrested may seek to use a weapon, or that evidence may be concealed or destroyed. To safeguard himself and others, and to prevent the loss of evidence, it has been held reasonable for the arresting officer to conduct a prompt, warrantless 'search of the arrestee's person and the area "within his immediate control" . . . .' [Citations.] [¶] Such searches may be conducted without a warrant, and they may also be made whether or not there is probable cause to believe that the person arrested may have a weapon or is about to destroy evidence. The potential dangers lurking in all custodial arrests make warrantless searches of items within the 'immediate control' area reasonable without requiring the arresting officer to calculate the probability that weapons or destructible evidence may be involved. [Citations.]" (*United States v. Chadwick* (1977) 433 U.S. 1, 14-15 (*Chadwick*).)[2]

---

[2] The area within an arrestee's immediate control is "'the area from within which [the arrestee] might gain possession of a

The People argue that the warrantless search in this case of the cell phone's text message folder was valid as a search incident to defendant's lawful arrest.[3] Defendant disagrees, arguing that the search "was too remote in time" to qualify as a valid search incident to his arrest.[4] In making this argument, he emphasizes that the phone "was exclusively held in police custody well before the search of its text message folder."

Resolution of this issue depends principally on the high court's decisions in *Robinson*, *Edwards*, and *Chadwick*. In *Robinson*, a police officer arrested the defendant for driving with a revoked operator's permit. (*Robinson*, *supra*, 414 U.S. at p. 220.) The officer conducted a patdown search and felt an object he could not identify in the breast pocket of the defendant's coat. He removed the object, which turned out to be a crumpled up cigarette package. He felt the package and determined it contained objects that were not cigarettes. He then opened the package and found 14 heroin capsules. (*Id.* at pp. 222-223.) The high court held that the warrantless search of the package was valid under the Fourth Amendment. (*Robinson*, *supra*, at p. 224.) It explained that, incident to a lawful custodial arrest, police have authority to conduct "a full search of the [arrestee's] person." (*Id.* at p. 235.) This authority, the court continued, exists whether or

---

weapon or destructible evidence.' [Citations.]" (*Chadwick*, *supra*, 433 U.S. at p. 14.)

[3] The People do not contest that defendant had a protected expectation of privacy in the contents of his text message folder. For purposes of this opinion, we therefore assume defendant had such an expectation, and do not consider the issue.

[4] Defendant does not question the legality of either his arrest or his phone's warrantless seizure. He challenges only the validity of the warrantless search of the phone's text message folder.

not the police have reason to believe the arrestee has on his or her person either evidence or weapons. "A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search [of the person] incident to the arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and . . . in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment." (*Ibid.*) Applying these principles, the court held: "The search of [the defendant's] person . . . and the seizure from him of the heroin, were permissible under established Fourth Amendment law. . . . Having in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it; and when his inspection revealed the heroin capsules, he was entitled to seize them as 'fruits, instrumentalities, or contraband' probative of criminal conduct. [Citations.]" (*Id.* at p. 236, fns. omitted.)

In *Edwards*, after lawfully arresting the defendant late one night for attempting to break into a post office, police took him to jail and placed him in a cell. (*Edwards*, *supra*, 415 U.S. at p. 801.) Ten hours later, suspecting that his clothes might contain paint chips from the window through which he had tried to enter, police made the defendant change into new clothes and held his old ones as evidence. (*Id.* at p. 802; see also *id.* at p. 810 (dis. opn. of Stewart, J.).) Subsequent examination of the old clothes revealed paint chips matching samples taken from the window. (*Id.* at p. 802.) The high court held that both the warrantless seizure of the clothes and the warrantless search of

them for paint chips were valid as a search incident to lawful arrest. (*Id.* at pp. 802-809.) It expressly rejected the argument that, because the search occurred "after the administrative mechanics of arrest ha[d] been completed and the prisoner [was] incarcerated," the search of the clothes was too remote in time to qualify as a search incident to arrest. (*Id.* at p. 804.) The court explained: "[O]nce the accused is lawfully arrested and is in custody, the effects in his possession at the place of detention that were subject to search at the time and place of his arrest may lawfully be searched and seized without a warrant *even though a substantial period of time has elapsed* between the arrest and subsequent administrative processing, on the one hand, and the taking of the property for use as evidence, on the other. This is true where the clothing or effects are immediately seized upon arrival at the jail, held under the defendant's name in the 'property room' of the jail, and at a later time searched and taken for use at the subsequent criminal trial. The result is the same where the property is not physically taken from the defendant until sometime after his incarceration." (*Id.* at pp. 807-808, fns. omitted, italics added.)

In *Chadwick*, *supra*, 433 U.S. 1, the high court cut back on the seemingly broad rule *Edwards* had announced. In *Chadwick*, federal narcotics agents observed the defendants load a 200-pound, double-locked footlocker into the trunk of a car. Having probable cause to believe the footlocker contained illegal contraband, the agents arrested the defendants and transported them to a federal building, along with the car and the footlocker. There, 90 minutes after the arrest and without obtaining a warrant or consent, the agents opened the footlocker and found marijuana

inside. (*Chadwick*, *supra*, at pp. 4-5.) The high court rejected the argument that the warrantless search was valid as a search incident to arrest. It first reaffirmed the principle that, because of "[t]he potential dangers lurking in all custodial arrests," police may conduct a warrantless search incident to arrest "whether or not there is probable cause to believe that the person arrested may have a weapon or is about to destroy evidence." (*Id.* at p. 14.) "However," the court explained, "warrantless searches of luggage or other property seized at the time of an arrest cannot be justified as incident to that arrest either if the 'search is remote in time or place from the arrest,' [citation], or no exigency exists. Once law enforcement officers have reduced luggage or other personal property *not immediately associated with the person of the arrestee* to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest." (*Id.* at p. 15, italics added.) Under this principle, the court held, because "the search was conducted more than an hour after federal agents had gained exclusive control of the footlocker and long after [the defendants] were securely in custody," it could not "be viewed as incidental to the arrest or as justified by any other exigency." (*Ibid.*) In reaching this conclusion, the court did not overrule *Robinson* or *Edwards*, but distinguished them as involving warrantless searches "of the person" rather than searches "of possessions within an arrestee's immediate control." (*Chadwick*, at p. 16, fn. 10.) The former searches, the court explained, are "justified by" the "reduced expectations of privacy caused by the arrest"; the latter are not. (*Ibid.*) Thus, the defendants'

"privacy interest in the contents of the footlocker was not eliminated simply because they were under arrest." (*Ibid.*)

Under these decisions, the key question in this case is whether defendant's cell phone was "personal property . . . immediately associated with [his] person" (*Chadwick*, *supra*, 433 U.S. at p. 15) like the cigarette package in *Robinson* and the clothes in *Edwards*. If it was, then the delayed warrantless search was a valid search incident to defendant's lawful custodial arrest. If it was not, then the search, because it was "'remote in time [and] place from the arrest,'" "cannot be justified as incident to that arrest" unless an "exigency exist[ed]."[5] (*Chadwick*, *supra*, at p. 15.)

We hold that the cell phone was "immediately associated with [defendant's] person" (*Chadwick*, *supra*, 433 U.S. at p. 15), and that the warrantless search of the cell phone therefore was valid. As the People explain, the cell phone "was an item [of personal property] on [defendant's] person at the time of his arrest and during the administrative processing at the police station." In this regard, it was like the clothing taken from the defendant in *Edwards* and the cigarette package taken from the defendant's coat pocket in *Robinson*, and it was unlike the footlocker in *Chadwick*, which was separate from the defendants' persons and was merely within the "area" of their "'immediate control.'" (*Chadwick*, *supra*, 433 U.S. at p. 15.) Because the cell phone was immediately associated with defendant's person, Fazio was

---

[5] The approximately 90-minute delay between defendant's arrest and the search of his cell phone was substantially similar to the 90-minute delay the high court held to be too remote in *Chadwick*.

"entitled to inspect" its contents without a warrant (*Robinson, supra*, 414 U.S. at p. 236) at the sheriff's station 90 minutes after defendant's arrest, whether or not an exigency existed.[6]

In arguing otherwise, defendant first asserts that, in deciding whether his cell phone is "the equivalent of" the cigarette package in *Robinson* or the footlocker in *Chadwick*, we should focus on its "character," not on the mere fact he was carrying it on his person. As defendant interprets the high court cases, a warrant is necessary for a delayed search unless the seized item is "clothing, or an article or container typically kept on or inside of clothing, or otherwise by its very nature carried on the arrestee's person." For two reasons, defendant argues, cell phones do not meet these criteria. First, they "are not necessarily or routinely[] worn, carried in a pocket, or attached to a person or his clothes," but are "more often kept *near* [their] owner[s], within [their] reach . . . inside a briefcase, backpack, or purse, or on a car seat or table, or

---

[6] Given our conclusion, we need not address the People's argument that an exigency existed because a cell phone's contents "are dynamic in nature and subject to change without warning – by the replacement of old data with new incoming calls or messages; by a mistaken push of a button; by the loss of power; by a person contacting the cellular phone provider; or by a person pre-selecting the 'cleanup' function on the cellular phone, which limits the length of time messages are stored before they are automatically deleted." We note, however, that the People have offered no evidence to support this claim. Nor have they offered evidence as to whether text messages deleted from a cell phone may be obtained from the cell phone's provider. (*See* Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence* (2010) 50 Santa Clara L. Rev. 183, 199 ["text messages are feasibly accessible for about two weeks from the cellular provider"].)

plugged into a power source, or stashed inside any manner of separate bags or carrying containers." Second, cell phones "contain[] quantities of personal data unrivaled by any conventional item of evidence traditionally considered to be 'immediately associated with the person of the arrestee,' such as an article of clothing, a wallet, or a crumpled cigarette box found in an arrestee's pocket," and therefore implicate heightened "privacy concerns" that warrant treating them "like . . . the footlocker in *Chadwick*."[7] The dissent endorses defendant's latter point, asserting that *all* cell phones should be exempt from the rule of *Robinson*, *Edwards*, and *Chadwick*, because the amount of personal information cell phones can store "dwarfs that which can be carried on the person in a spatial container." (Dis. opn. of Werdegar, J., *post*, at pp. 60a-61a.)

The relevant high court decisions do not support the view that whether police must get a warrant before searching an item they have properly seized *from an arrestee's person* incident to a lawful custodial arrest depends on the item's character, including its capacity for storing personal information. As noted above, *Chadwick* explains that a delayed warrantless search "of the person" (*Chadwick*, *supra*, 433 U.S. at p. 16, fn. 10) – which includes property "immediately associated with the person" at the time of arrest (*id.* at p. 15), but excludes property that is only "within an arrestee's immediate control" (*id.* at p. 16, fn. 10) – is

---

[7] Defendant's argument implicitly recognizes that courts commonly hold that delayed warrantless searches of wallets found on arrestees' persons are valid searches incident to arrest. (*See, e.g.*, *United States v. Passaro* (9th Cir. 1980) 624 F.2d 938, 943-944).

valid because of "reduced expectations of privacy caused by the arrest." (*Ibid.*) *Robinson* states that if a custodial arrest is lawful, then a "full" search of the arrestee's person "requires no additional justification." (*Robinson*, *supra*, 414 U.S. at p. 235.) *Edwards* states that "once the accused is lawfully arrested and is in custody, the effects in his possession at the place of detention that were subject to search at the time and place of his arrest may lawfully be searched and seized without a warrant even though a substantial period of time has elapsed between the arrest and subsequent administrative processing, on the one hand, and the taking of the property for use as evidence, on the other." (*Edwards*, *supra*, 415 U.S. at p. 807.) Nothing in these decisions even hints that whether a warrant is necessary for a search of an item properly seized from an arrestee's person incident to a lawful custodial arrest depends in any way on the character of the seized item.

Moreover, in analogous contexts, the high court has expressly rejected the view that the validity of a warrantless search depends on the character of the searched item. In *United States v. Ross* (1982) 456 U.S. 798, 825 (*Ross*), the court held that police who have probable cause to believe a lawfully stopped car contains contraband may conduct a warrantless search of any compartment or container in the car that may conceal the object of the search. As relevant here, the court stated that whether a particular container may be searched without a warrant does *not* depend on the character of the container, explaining: "[A] constitutional distinction between 'worthy' and 'unworthy' containers would be improper. Even though such a distinction perhaps could evolve in a series of cases in which paper bags, locked trunks, lunch

buckets, and orange crates were placed on one side of the line or the other, the central purpose of the Fourth Amendment forecloses such a distinction." (*Id.* at p. 822, fn. omitted.) "The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted."[8] (*Ross*, at p. 824.) In *New York v. Belton* (1981) 453 U.S. 454 (*Belton*), the court held that police making a lawful custodial arrest of a car's occupant "may, as a contemporaneous incident of that arrest," "examine the contents of *any* containers found within the passenger compartment." (*Id.* at p. 460, italics added.) As relevant here, the court rejected the proposition that whether a particular container may be searched without a warrant depends on the extent of the arrestee's reasonable expectation of privacy in that container, explaining: "[A]ny container[] . . . [in] the passenger compartment . . . may . . . be searched whether it is open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that *the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.*"[9] (*Belton*, at pp. 460-

---

[8] In reaching this conclusion, the high court in *Ross* rejected the view of several lower court judges who had concluded that, based on differing expectations of privacy, the warrantless search of a brown paper bag in Ross's stopped car was valid, but the warrantless search of a zippered leather pouch was not. (*Ross, supra*, 456 U.S. at p. 802.)

[9] In *Arizona v. Gant* (2009) 556 U.S. 332, 335, the high court limited *Belton, supra*, 453 U.S. 454, by holding that police may not search containers in a vehicle's passenger compartment "incident to a recent occupant's arrest after the arrestee has been secured and cannot access the interior of the vehicle," unless "it is reasonable to believe that evidence of the offense of arrest might be found in the vehicle." At the same time, the court reaffirmed

461, italics added.) Under *Ross*, *Belton*, and the other high court decisions discussed above, there is no legal basis for holding that the scope of a permissible warrantless search of an arrestee's person, including items immediately associated with the arrestee's person, depends on the nature or character of those items.

Regarding the particular focus of defendant and the dissent on the alleged storage capacity of cell phones, for several reasons, the argument is unpersuasive. First, the record contains no evidence regarding the storage capacity of cell phones in general or of defendant's cell phone in particular. Second, neither defendant nor the dissent persuasively explains why the sheer quantity of personal information should be determinative. Even "small spatial container[s]" (dis. opn. of Werdegar, J., *post*, at p. 54a) that hold less information than cell phones may contain highly personal, intimate and *private* information, such as photographs, letters, or diaries.[10]

Belton's holding that whether a particular container may be searched does not depend on its character or the extent of the arrestee's expectation of privacy in it. (*Gant*, 556 U.S. at p. 345 [in permissible warrantless search, police may search "every purse, briefcase, or other container within" the car's passenger compartment].) *Gant* is not otherwise relevant here, as it involved a search of the area within an arrestee's immediate control, not of the arrestee's person. (*Id.* at p. 335.)

[10] The dissent does not question that police may examine personal photographs found upon an arrestee's person, but objects that the high court has not held that police may read the contents of a letter or diary seized from an arrestee's person. (Dis. opn. of Werdegar, J., *post*, at p. 56a-57a, fn. 7.) However, several of the court of appeals decisions the high court in *Edwards* cited with approval on the issue of delayed searches (*Edwards*, *supra*, 415 U.S. at pp. 803-804, fn. 4) upheld the warrantless examination,

If, as the high court held in *Ross*, "a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf [has] an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case" (*Ross, supra*, 456 U.S. at p. 822), then travelers who carry sophisticated cell phones have no greater right to conceal personal information from official inspection than travelers who carry such information in "small spatial container[s]."[11] (Dis. opn. of Werdegar, J., *post*, at p. 54a) And if, as the high court held in *Belton*, differing expectations of privacy based on whether a container is open or closed are irrelevant to the validity of a warrantless search incident to arrest (*Belton, supra*, 453 U.S. at p. 461), then differing expectations of privacy based on the amount of information a particular item contains should also be irrelevant. Regarding the quantitative analysis of defendant and the dissent, the salient point of the high court's decisions is that a "lawful custodial arrest justifies the infringement of *any* privacy interest the arrestee may have" in property immediately associated

---

incident to arrest, of diaries or personal papers found upon the arrestee's person. (See *United States v. Gonzalez-Perez* (5th Cir. 1970) 426 F.2d 1283, 1285-1287 [papers contained in pockets, wallets, and purse]; *United States v. Frankenberry* (2d Cir. 1967) 387 F.2d 337, 339 [diary]; *Cotton v. United States* (9th Cir. 1967) 371 F.2d 385, 392 [papers contained in pockets]; *Grillo v. United States* (1st. Cir. 1964) 336 F.2d 211, 213 [paper contained in wallet].)

[11] Were the rule otherwise, those carrying small spatial containers, which are legally subject to seizure *and search* if found upon the person at the time of arrest, would find little solace in discovering that their intimate secrets would have been protected if only they had used a device that could hold more personal information.

with his or her person at the time of arrest (*ibid.*, italics added), even if there is no reason to believe the property contains weapons or evidence (*Robinson, supra*, 414 U.S. at p. 235). Third, even were it true that the amount of personal information *some* cell phones can store "dwarfs that which can be carried on the person in a spatial container" (dis. opn. of Werdegar, J., *post*, at pp. 60a-61a) – and, again, the record contains no evidence on this question – defendant and the dissent fail to explain why this circumstance would justify exempting *all* cell phones, including those with limited storage capacity, from the rule of *Robinson*, *Edwards*, and *Chadwick*.[12] A warrantless search, incident to a lawful arrest, of a cell phone with limited storage capacity does not become constitutionally unreasonable simply because other cell phones may have a significantly greater storage capacity.

Finally, adopting the quantitative approach of defendant and the dissent would create difficult line-drawing problems for both courts and police officers in the field. How would a court faced with a similar argument as to another type of item determine whether the item's storage capacity is constitutionally

---

[12] According to the United States Department of Justice, drug traffickers commonly use disposable cell phones, because they are relatively inexpensive and difficult to trace. (Nat. Drug Intelligence Center, U.S. Dept. J., Midwest High Intensity Drug Trafficking Area Drug Market Analysis 2009 (Mar. 2009) <http://www.justice.gov/ndic/pubs32/32775/distro.htm> [as of Jan. 3, 2011].) Such phones have limited storage capacity. (Ferro, *Cell phones: disposable mobile phone finally hits the US* (May 31, 2008) TECH.BLORGE Technology News <http://tech.blorge.com/Structure:%20/2008/05/31/cell-phones-disposable-mobile-phones-finally-hits-the-us/> [as of Jan. 3, 2011].)

significant? And how would an officer in the field determine this question upon arresting a suspect? Defendant and the dissent offer no guidance on these questions. Their approach would be "inherently subjective and highly fact specific, and would require precisely the sort of ad hoc determinations on the part of officers in the field and reviewing courts" that the high court has condemned. (*Thornton v. United States* (2004) 541 U.S. 615, 623; see also *Belton, supra*, 453 U.S. at pp. 458-459.) Similar concerns led the high court in *Robinson* to adopt the "straightforward," "easily applied, and predictably enforced" rule that "'a full [warrantless] search of the person'" is constitutionally permissible, and to "reject[] the suggestion that 'there must be litigated in each case the issue of whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest.' [Citation.]" (*Belton, supra*, 453 U.S. at p. 459, quoting *Robinson, supra*, 414 U.S. at p. 235.) Adopting the quantitative approach of defendant and the dissent, under which the validity of a warrantless search would turn on the amount of personal information a particular item might contain, would be contrary to these high court precedents. (See *United States v. Murphy* (4th Cir. 2009) 552 F.3d 405, 411 [in upholding warrantless search incident to arrest, refusing to distinguish cell phones based on their "large" storage capacity because of difficulty quantifying that term "in any meaningful way"].)

Defendant next argues that, in determining whether a warrant was necessary, we should distinguish between *the cell phone itself* and its *contents*. According to defendant, "[t]here is little about a cell phone's *content* that is conceptually linked

to or inextricably associated with the physical body or the inherent attributes of the arrestee's person. A cell phone's data content is not at all like a pair of pants or even a piece of paper folded up inside a wallet that has been tucked inside the pocket of a pair of pants." It "cannot be worn or 'carried' on one's person." "[T]he nature of the evidence that a cell phone may contain, and the fact that the cell phone 'container' is readily differentiated from the cell phone 'content,' warrants treating the cell phone content differently from the seized cell phone itself." The dissent makes a similar argument, distinguishing between "the arrestee's actual person" and the cell phone's content – i.e., the stored data – and arguing that the loss of "*bodily* privacy" that justifies a warrantless "search of an arrestee's person" upon arrest does not also justify the search of a cell phone found upon the arrestee's person. (Dis. opn. of Werdegar, J., *post*, at pp. 63a-63a.)

These arguments are inconsistent with the high court's decisions. Those decisions hold that the loss of privacy upon arrest extends beyond the arrestee's body to include "personal property . . . immediately associated with the person of the arrestee" at the time of arrest. (*Chadwick*, *supra*, 433 U.S. at p. 15.) They also hold, contrary to the dissent's suggestion, that this loss of privacy entitles police not only to "seize" anything of importance they find on the arrestee's body (dis. opn. of Werdegar, J., *post*, at p. 63a.), but also *to open and examine* what they find. Thus, the court in *Robinson* held that a police officer, despite seizing a cigarette package from the defendant's shirt pocket and reducing it to police control, did not need to obtain a warrant before opening the package and examining its contents. (*Robinson*, *supra*, 414 U.S. at

p. 236.) Similarly, the court in *Edwards* held that the police, despite seizing the defendant's clothes and reducing them to police control, did not need to obtain a warrant before subjecting those clothes to laboratory testing. (*Edwards*, *supra*, 415 U.S. at pp. 802-809.) In both cases, the high court expressly refused to distinguish the contents of the seized item from either the seized item itself or "the arrestee's actual person." (Dis. opn. of Werdegar, *post*, at p. 64a.) As the court later explained in *Belton* in refusing to draw a constitutional distinction between the seizure of an item and a search of that item: "[U]nder this fallacious theory, no search or seizure incident to a lawful custodial arrest would ever be valid; by seizing an article even on the arrestee's person, an officer may be said to have reduced that article to his [or her] 'exclusive control.'" (*Belton*, *supra*, 453 U.S. at pp. 461-462, fn. 5.) Under these high court decisions, in determining the validity of a search incident to arrest, there is no legal basis for distinguishing the contents of an item found upon an arrestee's person from either the seized item itself or "the arrestee's actual person."[13] (Dis. opn. of Werdegar, J., *post*, at p. 64a.)

---

[13] Defendant insists that *Edwards* is "limited by its facts to the delayed search of an article of clothing." However, the court's discussion more broadly addressed "other belongings" (*Edwards*, *supra*, 415 U.S. at p. 804) and "effects in [the arrestee's] possession" (*id.* at p. 807). We do not consider ourselves free to disregard this discussion, especially in light of *Robinson*, which did not involve clothing, and *Chadwick*, which reaffirmed the validity of delayed warrantless searches of "personal property . . . immediately associated with the person of the arrestee." (*Chadwick*, *supra*, 433 U.S. at p. 15.) Defendant alternatively suggests that *Edwards* validates delayed warrantless searches only of "'effects still in the defendant's possession at the place of detention, such as the defendant's clothing.'" Again, the high

The dissent makes several arguments in addition to defendant's, but they are also unpersuasive. Although conceding that *Robinson*, *Edwards*, and *Chadwick*, "reasonably read," authorize delayed warrantless searches "of containers" immediately associated with an arrestee's person, the dissent asserts that cell phones are exempt from this rule because they are not "'containers' within the meaning of the high court's search decisions." (Dis. opn. of Werdegar, J., *post*, at p. 62a.) However, application of the rule of *Robinson*, *Edwards*, and *Chadwick* turns not on whether the item in question constitutes a "container," but on whether it is "property," *i.e.*, a "belonging[]" or an "effect[]."[14] (*Edwards*, *supra*, 415 U.S. at pp. 803-804, 807-808; see also *Chadwick*, *supra*, 433 U.S. at p. 15; *Robinson*, *supra*, 414 U.S. at pp. 229, 232.) The dissent's attempt to limit the reach of that rule to "clothing and small spatial containers" (dis. opn. of Werdegar, J., *post*, at p. 61a) finds no support in the language of the high court's governing decisions. In this respect, the language of those decisions is entirely consistent with the Fourth Amendment itself, which protects "[t]he right of the people to be secure in their persons, houses, papers, *and effects*." (Italics added.) It is also consistent with

---

court's opinion is not so limited; the court stated that a delayed warrantless search is valid "where the clothing or effects are immediately seized upon arrival at the jail, held under the defendant's name in the 'property room' of the jail, and at a later time searched and taken for use at the subsequent criminal trial." (*Edwards*, *supra*, at p. 807.)

[14] The word "container" does not appear in *Robinson* and *Edwards*. It appears once in *Chadwick*, in a footnote where the high court explained that the defendant's principal privacy interest in the footlocker was "not in the container itself . . . but in its contents." (*Chadwick*, *supra*, 433 U.S. at pp. 13-14, fn. 8.)

one of the justifications for the search incident to arrest exception: "the reasonableness of searching for . . . *evidence* of crime when a person is taken into official custody and lawfully detained. [Citation.]" (*Edwards*, *supra*, 415 U.S. at pp. 802-803, italics added.) Contrary to the dissent's analysis, whether an item of personal property constitutes a "container" bears no relation to this justification.[15]

The dissent also errs in asserting that the high court's "rationale" for allowing delayed warrantless searches incident to arrest is of "doubtful" applicability to "items that are easily removed from the arrestee's possession and secured by the police." (Dis. opn. of Werdegar, J., *post*, at p. 58a.) In *Edwards*, the high court declared it "plain that searches and seizures that [may] be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention." (*Edwards*, *supra*, 415 U.S. at p. 803.) The rationale for this rule, the court explained, is that the arrestee is "no more imposed upon" by a delayed search "than he [or she] could have been" by a warrantless search "at the time and place of the arrest. . . ." (*Id.* at p. 805.) There is "little difference," the court reasoned, between conducting the search at

---

[15] The high court did discuss containers in the decisions we have cited as involving "analogous contexts." (*Ante*, at pp. 10-12.) In this respect, our analysis is consistent with the weight of authority. (*State v. Boyd* (Conn. 2010) 992 A.2d 1071, 1089, fn. 17 ["A number of courts have analogized cell phones to closed containers and concluded that a search of their contents is, therefore, valid under the automobile exception or the exception for a search incident to arrest."].) Moreover, contrary to the dissent's analysis, nothing in these analogous decisions purports to limit the rule of *Robinson*, *Edwards*, and *Chadwick* to property that classifies as a container.

the place of arrest and conducting it later at the place of detention. (*Id.* at p. 803.) This analysis is consistent with the high court's earlier statement in *Robinson* that "[a] police officer's determination as to how *and where* to search the person of a suspect whom he has arrested is necessarily a quick *ad hoc* judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search." (*Robinson*, *supra*, 414 U.S. at p. 235, first italics added.) It is also consistent with the high court's subsequent statement in *Chadwick* that a delayed warrantless search of personal property immediately associated with the person of an arrestee at the time of arrest is justified by the "reduced expectations of privacy caused by the arrest." (*Chadwick*, *supra*, 433 U.S. at p. 16, fn. 10.) Contrary to the dissent's assertion, the rationale of these decisions – that a delayed search of an item of personal property found upon an arrestee's person no more imposes upon the arrestee's constitutionally protected privacy interest than does a search at the time and place of arrest – fully applies to the delayed search of defendant's cell phone.[16]

---

[16] Not satisfied with the high court's explicit explanations, the dissent, citing just two of the 20 court of appeals decisions *Edwards* string-cited on the point (see *Edwards*, *supra*, 415 U.S. at pp. 803-804, fn. 4), asserts that the high court's "rationale is to avoid logistically awkward or embarrassing public searches." (Dis. opn. of Werdegar, J., *post*, at p. 58a.) This assertion finds no support in the language of the high court's decisions, no doubt because making the validity of a delayed search turn on the logistics or potential embarrassment of a public search would, like the dissent's quantitative approach, require "the sort of ad hoc determinations on the part of officers in the field and reviewing courts" that the high court has condemned. (*Thornton v. U.S.*, *supra*, 541 U.S. at p. 623.)

For the reasons discussed above, we hold that, under the United States Supreme Court's binding precedent, the warrantless search of defendant's cell phone was valid. If, as the dissent asserts, the wisdom of the high court's decisions "must be newly evaluated" in light of modern technology (dis. opn. of Werdegar, J., *post*, at p. 52a), then that reevaluation must be undertaken by the high court itself.[17]

DISPOSITION

The judgment of the Court of Appeal is affirmed.

CHIN, J.

---

[17] Only a few published decisions exist regarding the validity of a warrantless search of a cell phone incident to a lawful custodial arrest. Most are in accord with our conclusion. (*See, e.g., United States v. Murphy, supra*, 552 F.3d at p. 412 [citing *Edwards* in holding that "once [the defendant's] cell phone was held for evidence, other officers and investigators were entitled to conduct a further review of its contents . . . without seeking a warrant"]; *United States v. Finley* (5th Cir. 2007) 477 F.3d 250, 260, fn. 7 [arrestee's cell phone "does not fit into [*Chadwick*'s] category of 'property not immediately associated with [his] person' because it was on his person at the time of his arrest"]; *United States v. Wurie* (D. Mass. 2009) 612 F. Supp. 2d 104, 110 [upholding delayed search of cell phone, finding "no principled basis for distinguishing a warrantless search of a cell phone from the search of other types of personal containers found on a defendant's person that" have been upheld under *Edwards*].)

In a closely divided (four to three) opinion, the Supreme Court of Ohio held otherwise, reasoning that "because a person has a high expectation of privacy in a cell phone's contents," police, after seizing a cell phone from an arrestee's person, "must . . . obtain a warrant before intruding into the phone's contents." (*State v. Smith* (Ohio 2009) 920 N.E.2d 949, 955.) The Ohio court's focus on the extent of the arrestee's expectation of privacy is, as previously explained, inconsistent with the high court's decisions.

WE CONCUR:

KENNARD, Acting C.J.
BAXTER, J.
CORRIGAN, J.
GEORGE, J.*

---

* Retired Chief Justice of California, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

CONCURRING OPINION BY KENNARD, ACTING C.J.

The majority holds that the police may, without obtaining a warrant, view or listen to information electronically stored on a mobile phone that a suspect was carrying when lawfully arrested. The dissent disagrees. I explain why I join the majority rather than the dissent.

On June 8, 1982, California voters enacted an initiative measure known as Proposition 8. Among other things, Proposition 8 added to the California Constitution a "Right to Truth-in-Evidence" provision (Cal. Const., art. 1, § 28, former subd. (d) [now subd. (f)(2)]). That provision generally prohibits exclusion of relevant evidence in a criminal proceeding on the ground that the evidence was obtained unlawfully. Because the federal Constitution is "the supreme law of the land" (U.S. Const., art. VI, § 2), and thus prevails over conflicting state constitutional provisions, the state Constitution's "Right to Truth-in-Evidence" provision does not apply when relevant evidence must be excluded because it was obtained in violation of the federal Constitution's Fourth Amendment, which prohibits "unreasonable searches and seizures." As a result, in California criminal proceedings all issues related to the suppression of evidence derived from police searches and seizures are now determined by application of federal constitutional law. (*People v. Lenart* (2004) 32 Cal. 4th 1107, 1118; *People v. Sapp* (2003) 31 Cal. 4th 240, 267; *People v. Bradford* (1997) 15 Cal. 4th 1229, 1291.) On issues of federal constitutional law, the decisions of the United States Supreme Court are controlling. (*Gates v.*

Discovery Communications, Inc. (2004) 34 Cal. 4th 679, 692.)

As the majority explains, three decisions of the United States Supreme Court compel the result in this case. Those decisions are *United States v. Robinson* (1973) 414 U.S. 218 (*Robinson*), *United States v. Edwards* (1974) 415 U.S. 800 (*Edwards*), and *United States v. Chadwick* (1977) 433 U.S. 1 (*Chadwick*). Under *Robinson* and *Chadwick*, a warrant is not required to conduct a "full search of the person" incident to a lawful arrest (*Robinson*, at p. 235), and the police may examine an object found during the search to determine whether it contains evidence of crime (*id.* at p. 236), so long as the object is one that is "immediately associated with the person of the arrestee" (*Chadwick*, at p. 15). Under *Edwards*, this search and inspection need not occur at the time and place of the arrest; it may occur even after "a substantial period of time has elapsed." (*Edwards*, at p. 807.)

When carried in clothing (rather than inside luggage or a similar container), a mobile phone is personal property that is "immediately associated with the person of the arrestee" (*Chadwick*, *supra*, 433 U.S. 1, 15). Accordingly, under controlling high court decisions, police may, without obtaining a warrant, inspect a mobile phone carried by a suspect at the time of arrest, by viewing or listening to its electronically stored data, including text messages, even when a substantial time has elapsed since the arrest.

The dissent asserts that in light of the vast data storage capacity of "smart phones" and similar devices, the privacy interests that the federal Constitution's Fourth Amendment was intended to protect would be

better served by a rule that did not allow police "to rummage at leisure through the wealth of personal and business information that can be carried on a mobile phone or handheld computer merely because the device was taken from an arrestee's person." (Dis. opn., *post*, at p. 65a.) The dissent also asserts that the three high court decisions I have mentioned are not binding here because they "were not made with mobile phones, smartphones and handheld computers – none of which existed at the time – in mind." (Dis. opn., *post*, at p. 61a.) In my view, however, the recent emergence of this new technology does not diminish or reduce in scope the binding force of high court precedents.

I join the majority rather than the dissent because the United States Supreme Court has cautioned that on issues of federal law all courts must follow its directly applicable precedents, even when there are reasons to anticipate that it might reconsider, or create an exception to, a rule of law that it has established. (*Rodriguez de Quijas v. Shearson/Am. Exp.* (1989) 490 U.S. 477, 484.) The high court has reserved to itself alone "the prerogative of overruling its own decisions." (*Ibid.*; see *Scheiding v. General Motors Corp.* (2000) 22 Cal. 4th 471, 478.)

Under the compulsion of directly applicable United States Supreme Court precedent, I join the majority in affirming the Court of Appeal's judgment.

KENNARD, ACTING C. J.

DISSENTING OPINION BY WERDEGAR, J.

I respectfully dissent. The majority concludes police may search the data stored on an arrestee's mobile phone without a warrant, as they may search clothing (see *United States v. Edwards* (1974) 415 U.S. 800 (*Edwards*)) or small physical containers such as a crumpled cigarette package (see *United States v. Robinson* (1973) 414 U.S. 218 (*Robinson*)) taken from the person of an arrestee. In my view, electronic communication and data storage devices carried on the person – cellular phones, smartphones and handheld computers – are not sufficiently analogous to the clothing considered in *Edwards* or the crumpled cigarette package in *Robinson* to justify a blanket exception to the Fourth Amendment's warrant requirement. A particular context-dependent balancing of constitutionally protected privacy interests against the police interests in safety and preservation of evidence led the United States Supreme Court, over 30 years ago, to hold searches of the arrestee's person reasonable despite the lack of probable cause or a warrant and despite substantial delay between the arrest and the search. (See *United States v. Chadwick* (1977) 433 U.S. 1, 14-15 (*Chadwick*).) Today, in the very different context of mobile phones and related devices, that balance must be newly evaluated.[1]

---

[1] The separately concurring justice correctly observes that we must follow directly applicable decisions from the United States Supreme Court even if we think them due for reexamination. (*Rodrigues de Quijas v. Shearson/Am. Exp.* (1989) 490 U.S. 477, 484.) But where high court precedent is not on all fours with the case at bar, we also must remember that the language of Supreme Court decisions is to "be read in the light of the facts of the case under discussion" and that "[g]eneral expressions transposed to other facts are often misleading." (*Armour & Co. v.*

The potential intrusion on informational privacy involved in a police search of a person's mobile phone, smartphone or handheld computer is unique among searches of an arrestee's person and effects. A contemporary smartphone[2] can hold hundreds or thousands of messages, photographs, videos, maps, contacts, financial records, memoranda and other documents, as well as records of the user's telephone calls and Web browsing.[3] Never before has it been

---

Wantock (1944) 323 U.S. 126, 133.) Indeed, the Supreme Court recently emphasized that *stare decisis* should not be used "to justify the continuance of an unconstitutional police practice. . . . in a case that is so easily distinguished from the decisions that arguably compel it." (*Arizona v. Gant* (2009) 556 U.S. 332, 348.)

The facts of the present case, as I will explain, differ in important respects from those that gave rise to the United States Supreme Court decisions in *Robinson*, *Edwards* and *Chadwick*. These precedents, therefore, provide no basis for evading this court's independent responsibility to determine the constitutionality of the search at issue. While we of course have no authority to overrule them, we may and should refrain from applying their language blindly to new and fundamentally different factual circumstances.

[2] PCMag.com's online encyclopedia defines a smartphone as "[a] cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as text messaging, e-mail, Web browsing, still and video cameras, MP3 player and video and TV viewing. In addition to their built-in functions, smartphones can run myriad applications, turning the once single-minded cellphone into a mobile computer." (<http://www.pcmag.com/encyclopedia_term/0,2542,%20t=Smartphone&i=51537,00.asp> [as of Jan. 3, 2011].)

[3] Apple's iPhone 4, HTC's Droid Incredible, and the BlackBerry Torch all can store up to 32 gigabytes of data, which could include thousands of images or other digital files. (*See* <http://www.apple.com/iphone/specs.html>; <http://www.htc.com/us/products/droid-incredible-verizon?view=1-1&sort=0#tech-specs>; and <http://us.blackberry.com/smartphones/

possible to carry so much personal or business information in one's pocket or purse. The potential impairment to privacy if arrestees' mobile phones and handheld computers are treated like clothing or cigarette packages, fully searchable without probable cause or a warrant, is correspondingly great.

Although the record does not disclose the type of mobile phone defendant possessed, I discuss smartphones as well as other mobile phones for two reasons. First, the rule adopted by the majority – that an electronic device carried on the person is for Fourth Amendment purposes indistinguishable from an individual's clothing or a small spatial container – is broad enough to encompass all types of handheld electronic data devices, including smartphones such as iPhones and BlackBerry devices, as well as other types of handheld computers. While I disagree with the majority's holding on the validity of the search here, I agree that the permissibility of a search incident to arrest should not depend on the features or technical specifications of the mobile device, which could be difficult to determine at the time of arrest.[4] Second, smartphones make up a growing share of the United States mobile phone market and are likely to be pervasive in the near future. (See Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra*, 56

---

blackberrytorch/#!phone-specifications> [all as of Jan. 3, 2011].) On the capabilities of smartphones generally, *see* Gershowitz, *The iPhone Meets the Fourth Amendment* (2008) 56 UCLA L. Rev. 27, 29-30.

[4] But *see* Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence* (2010) 50 Santa Clara L. Rev. 183, 222 (proposing to distinguish smartphones from "older generation cellular phones" by presence of a touch screen or full keyboard, and to impose stricter limits on searches of smartphones).

UCLA L. Rev. at p. 29 ["It does not take a crystal ball to predict that such devices will be ubiquitous in the United States within a few years."].)[5] The question of when and how they may be searched is therefore an important one.

Warrantless searches incident to arrest are justified by the important interests in officer safety and preservation of evidence. "When a custodial arrest is made, there is always some danger that the person arrested may seek to use a weapon, or that evidence may be concealed or destroyed. To safeguard himself and others, and to prevent the loss of evidence, it has been held reasonable for the arresting officer to conduct a prompt, warrantless 'search of the arrestee's person and the area "within his immediate control"–construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.'" (*Chadwick*, *supra*, 433 U.S. at p. 14, quoting *Chimel v. California* (1969) 395 U.S. 752, 763.)

Weapons, of course, may be hidden in an arrestee's clothing or in a physical container on the person. But there is apparently no "app" that will turn an iPhone or any other mobile phone into an effective weapon for use against an arresting officer (and if there were,

---

[5] In the third quarter of 2010 alone, for example, more than 20 million smartphones were reportedly sold in the United States, up from about 14.5 million in the second quarter of 2010 and 9.7 million in the same quarter of 2009. (Bilton, *The Race to Dominate the Smartphone Market*, N.Y. Times Bits Blog (Nov. 1, 2010) <http://bits.blogs.nytimes.com/2010/11/01/apple-and-google-excel-in-u-s-smartphone-growth/> [as of Jan. 3, 2011]; Hamblen, *OS War Has Android on Top in U.S. Smartphone Sales* (Aug. 12, 2010) Computerworld <http://www.computerworld.com/s/article/9180624/OS_war_has_Android_on_top_in_U.S._smartphone_sales> [as of Jan. 3, 2011].)

officers would presumably seek to disarm the phone rather than search its data files). Clearly, any justification for the warrantless search of a mobile phone must come from the possibility that the arrestee might, during the arrest, destroy evidence stored on the phone.

Once a mobile phone has been seized from an arrestee and is under the exclusive control of the police, the arrestee, who is also in police custody, cannot destroy any evidence stored on it.[6] At that point a search of its stored data would seem to require a warrant, for "when no exigency is shown to support the need for an immediate search, the Warrant Clause places the line at the point where the property to be searched comes under the exclusive dominion of police authority." (*Chadwick*, *supra*, 433 U.S. at p. 15.) As the majority notes (maj. opn., *ante*, at p. 34a, fn. 6), no evidence of exigency was presented in this case – no evidence that the text messages on defendant's phone were subject to imminent loss and could not, in any event, be obtained from defendant's cellular provider.[7]

---

[6] Defendant did not challenge the seizure of his phone, only the search of the data stored on it. Nor do I contend the police needed a warrant or probable cause to take defendant's phone from him and secure it. Once secured, the phone could have been searched later if a warrant, founded on probable cause, issued for the search.

[7] At oral argument, the Attorney General noted that data on some smartphones can be remotely wiped, which might allow an accomplice to destroy evidence on the phone even while the arrestee remains in custody and the phone in police control. As an argument for warrantless searching, this proves too much. A suspect arrested in his or her home or office might also leave behind a computer with evidence that could be destroyed by an accomplice while the arrestee is in custody, but this possibility does not entitle police to search the contents of such computers

We are left, then, with the claim, accepted by the majority, that a mobile phone, like clothing and other items carried on the arrestee's person, may, under *Edwards*, be searched without a warrant even after the item has been secured and the suspect taken into custody, if it could have been searched at the time and place of arrest. (*See Edwards, supra*, 415 U.S. at pp. 803-804, 807-808.) As to clothing and small physical containers, the law, in effect, indulges a fiction that an item that was on the arrestee's person when he was detained is *still* on his person – and thus vulnerable to destruction of evidence – notwithstanding that the arrestee is safely in custody and the item securely in police control. (*See New York v. Belton* (1981) 453 U.S. 454, 466 (dis. opn. of Brennan, J.) [characterizing holding in *Belton*, which allowed a vehicle interior to be searched incident to arrest, as resting on "a fiction – that the interior of a car is *always* within the immediate control of an arrestee who has recently been in the car"]; Butterfoss, *As Time Goes By: The Elimination of Contemporaneity and Brevity as Factors in Search and Seizure Cases* (1986) 21 Harv. C.R.-C.L. L. Rev. 603, 625 [broadly read, *Edwards* represented a "radical shift" in approach to the

---

without probable cause or a search warrant. In either circumstance (home computer or handheld computer) an immediate search without waiting for a warrant might be desirable from the perspective of efficient policing, but "the mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." (*Mincey v. Arizona* (1978) 437 U.S. 385, 393.) In any event, it appears that remote wiping can be avoided by removing the smartphone's battery and/or storing the phone in a shielded container, as law enforcement officers are being trained to do. (*See* Grubb, *Remote Wiping Thwarts Secret Service*, ZDNet (Australian ed., May 18, 2010) <http://www.zdnet.com.au/remote-wiping-thwarts-secret-service-339303239.htm> [as of Jan. 3, 2011].)

delayed-search problem, by which an exigency exception to the traditional contemporaneity rule displaced the rule itself].)

Beyond observing that the defendant in *Edwards* "was no more imposed upon" than if his clothes had been taken from him earlier (*Edwards, supra*, 415 U.S. at p. 805), the *Edwards* court did not explain its reasons for allowing delayed warrantless searches incident to arrest. In particular, the high court did not explain what police interest *justified* a delayed warrantless search once the arrestee and his or her effects are safely in police control. But court of appeals decisions cited by the high court (*id.* at pp. 803-804, fn. 4) suggest the rationale is to avoid logistically awkward or embarrassing public searches. (*See United States v. Gonzalez-Perez* (5th Cir. 1970) 426 F.2d 1283, 1287 ["The arresting officers are not required to stand in a public place examining papers or other evidence on the person of the defendant in order for such evidence to be admissible."]; *United States v. DeLeo* (1st Cir. 1970) 422 F.2d 487, 493 ["Were this not to be so, every person arrested for a serious crime would be subjected to thorough and possibly humiliating search where and when apprehended."].) This rationale makes sense as to an arrestee's actual person or clothing – the issue in *Edwards* – but its applicability to items that are easily removed from the arrestee's possession and secured by the police, such as mobile phones, is doubtful. With such items the police choices are not limited to an awkward or cursory on-the-spot search or a thorough warrantless search at the station house. Rather, the item can be taken from the arrestee and securely held until (assuming probable cause for a search exists) a warrant has issued. (*See United States v. Monclavo-Cruz* (9th Cir.

1981) 662 F.2d 1285, 1288 [delayed warrantless search of purse held unreasonable: "The fact that an officer is prevented from conducting a *Chimel/Belton* search, however, is not a sufficient reason to justify a search an hour later at the station. The protective rationale for the search no longer applies."].)

Recently, addressing the search of an arrestee's vehicle, the high court rejected the fictional approach to justification of a search incident to arrest, holding instead "that the *Chimel* rationale authorizes police to search a vehicle incident to a recent occupant's arrest only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." (*Arizona v. Gant, supra*, 556 U.S. at p. 343.) Just as the court in *Gant* adopted a narrow reading of *New York v. Belton, supra*, 453 U.S. 454, so, too, some courts and commentators have suggested a narrow reading of *Edwards*, in which delayed searches incident to arrest would be per se valid only as to the arrestee's actual person or clothing (which cannot easily be separated from the person at the time of arrest). (*See United States v. Schleis* (8th Cir. 1978) 582 F.2d 1166, 1171 [disapproving station house search of arrestee's locked briefcase]; Butterfoss, *As Time Goes By: The Elimination of Contemporaneity and Brevity as Factors in Search and Seizure Cases, supra*, 21 Harv. C.R.-C.L. L. Rev. at p. 626 [noting possibility of reading *Edwards* as dependent on impossibility of taking arrestee's clothes until replacement clothes were available at the jail].) Indeed, the defendant in *Edwards* had objected, and the court of appeals had reversed his conviction, only on grounds that the delayed warrantless seizure of *his clothing* violated the Fourth Amendment to the United States Constitution. (*Edwards, supra*, 415 U.S. at p.

802, italics added.) No issue was presented as to the delayed warrantless seizure or search of *a container* carried by an arrestee.

Edwards nonetheless spoke broadly, and *Chadwick* suggests items beyond clothing may be subject to delayed warrantless search if they are "immediately associated with the person of the arrestee." (*Chadwick*, *supra*, 433 U.S. at p. 15; see also *id.* at p. 16, fn. 10 [describing *Robinson* (which involved search of a small container), as well as *Edwards*, as a search "of the person"].) The majority thus reasonably reads existing high court authority as permitting delayed warrantless searches of containers immediately associated with an arrestee's person.

The question is whether the information stored on electronic devices such as mobile phones, as at issue here, may be examined without a warrant under the same rationale. For two reasons, I would hold it may not.

First, as suggested earlier, the amount and type of personal and business information that can be stored on a mobile phone, smartphone or handheld computer, and would become subject to delayed warrantless search under the majority holding, dwarfs that which can be carried on the person in a spatial container.[8] As one federal district court observed in suppressing the fruits of a mobile phone search, "modern cellular phones have the capacity for storing immense amounts

---

[8] The majority observes that substantial private information can be carried in the nondigital forms of letters and diaries. (Maj. opn., *ante*, at pp. 38a-39a.) Implicit in the majority's argument is the assumption that police may not only take a letter or diary from an arrestee and inventory it, but may, without a warrant, read through all of its contents. Neither this court nor the United States Supreme Court has so held.

of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages." (*United States v. Park* (N.D. Cal., May 23, 2007, No. CR 05-375 SI) 2007 U.S. Dist. Lexis 40596, *21-*22, fn. omitted.) Smartphones, as we have seen, have even greater information storage capacities.

The United States Supreme Court's holdings on clothing and small spatial containers were not made with mobile phones, smartphones and handheld computers – none of which existed at the time – in mind. Electronic devices "contain" information in a manner very different from the way the crumpled cigarette package in *Robinson* contained capsules of heroin. (*See Robinson, supra*, 414 U.S. at p. 223.) Electronic devices, indeed, are not even "containers" within the meaning of the high court's search decisions. As the Ohio Supreme Court, rejecting application of the container cases to a mobile phone, noted, "[o]bjects falling under the banner of 'closed container' have traditionally been physical objects capable of holding other physical objects. Indeed, the United States Supreme Court has stated that in this situation, 'container' means 'any object capable of holding another object.'" (*State v. Smith* (Ohio 2009) 920 N.E.2d 949, 954, quoting *New York v. Belton, supra*, 453 U.S. at p. 460, fn. 4.)[9]

---

[9] The *Belton* court stated: "'Container' here denotes any object capable of holding another object. It thus includes closed or open glove compartments, consoles, or other receptacles located

Second, the grounds for deeming an arrestee to have lost privacy rights in his or her *person* do not apply to the privacy interest in *data* stored on electronic devices. In *Robinson*, the Supreme Court, quoting with approval from a New York case, explained that while warrantless searches of the person are ordinarily unlawful, "'[s]earch of the person becomes lawful when grounds for arrest and accusation have been discovered, and *the law is in the act of subjecting the body of the accused to its physical dominion.*'" (*Robinson*, *supra*, 414 U.S. at p. 232, italics added.) In *Edwards*, the court reasoned that where the state has lawfully taken a person into custody, though not all his privacy interests are destroyed, the arrest "'does – for at least a reasonable time and to a reasonable extent – take *his own privacy* out of the realm of protection from police interest in weapons, means of escape, and evidence.'" (*Edwards*, *supra*, 415 U.S. at pp. 808-809, italics added.) Citing *Robinson* and *Edwards*, the court subsequently distinguished "searches of the person," in which the

---

anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like." (*New York v. Belton*, *supra*, 453 U.S. at pp. 460-461, fn. 4.) As *Belton* clearly spoke only of objects physically containing other objects, the majority's reliance on that case for the proposition that any "container," whatever the extent of the arrestee's expectation of privacy in it, may be searched incident to arrest (maj. opn., *ante*, at p. 11) is misplaced when it comes to mobile phones and other electronic communication and data storage devices. Still less on point is *United States v. Ross* (1982) 456 U.S. 798, which did not even involve a search incident to arrest. That the high court in *Ross* declined to distinguish among probable cause searches of "paper bags, locked trunks, lunch buckets, and orange crates" carried in automobiles (*id.* at p. 822) hardly requires that an arrestee's mobile phone, smartphone or handheld computer be treated the same as clothing or a crumpled cigarette package.

arrest created a "reduced expectation[] of privacy," from searches of the possessions within an arrestee's control. (*Chadwick*, *supra*, 433 U.S. at p. 16, fn. 10.)

The warrantless search of an arrestee's person thus rests on a relatively simple, intuitively correct idea: the police, having lawful custody of the individual, necessarily have the authority to search the arrestee's body and seize anything of importance they find there. Having been lawfully arrested, with his or her person under the custody and control of the police, the individual can no longer claim in full the personal privacy he or she ordinarily enjoys. It does not follow, however, that the police also have "'dominion'" (*Robinson*, *supra*, 414 U.S. at p. 232) over the entirety of stored messages, photographs, videos, memoranda and other records an arrestee may be carrying on a mobile phone or smartphone. An individual lawfully arrested and taken into police custody necessarily loses much of his or her *bodily* privacy, but does not necessarily suffer a reduction in the *informational* privacy that protects the arrestee's records. That an arrestee's interest in his or her "'own privacy'" (*Edwards*, *supra*, 415 U.S. at p. 809) is severely reduced does not imply a corresponding reduction in privacy of personal and business data. Even when they happen to be stored on a device carried on the person, these records are clearly distinct from the person of the arrestee.

Because the data stored on a mobile phone or other electronic device is easily distinguished from the arrestee's actual person, and in light of the extraordinary potential for invasion of informational privacy involved in searching data stored on such devices, I would hold mobile phones, smartphones and handheld computers are not ordinarily subject to

delayed, warrantless search incident to arrest. In the terms provided by the existing United States Supreme Court authority, search of the information stored on an arrestee's mobile phone or similar device should be treated as the search of an item "within an arrestee's immediate control" rather than a search "of the person." (*Chadwick, supra*, 433 U.S. at p. 16, fn. 10.) Once an arrestee's mobile phone or similar device is securely "under the exclusive dominion of police authority" (*id.* at p. 15), the arrest itself no longer serves to authorize a warrantless search of its stored data.

This is not to say police may never examine or search an arrestee's mobile phone without a warrant. Devices carried on the arrestee's person may be seized and secured. Some examination of the device, not amounting to a search of its data folders, might also be reasonable. (*See, e.g., United States v. Wurie* (D. Mass. 2009) 612 F. Supp. 2d 104, 106-107 [when arrestee's mobile phone rang, officer flipped it open and observed originating number and "wallpaper" photograph, which led to discovery of arrestee's residence address].) And where the arresting officers have reason to fear imminent loss of evidence from the device, or some other exigency makes immediate retrieval of information advisable, warrantless examination and search of the device would be justified. (*See, e.g., United States v. Lottie* (N.D. Ind., Jan. 14, 2008, No. 3:07cr51RM) 2008 U.S. Dist. Lexis 2864, *9 [officers had reason to believe that accomplices in large drug transaction, "unknown but potentially present and armed," were conducting countersurveillance of the police operation, raising concern for safety of officers and the public].)

The majority's holding, however, goes much further, apparently allowing police carte blanche, with no showing of exigency, to rummage at leisure through the wealth of personal and business information that can be carried on a mobile phone or handheld computer merely because the device was taken from an arrestee's person. The majority thus sanctions a highly intrusive and unjustified type of search, one meeting neither the warrant requirement nor the reasonableness requirement of the Fourth Amendment to the United States Constitution. As a commentator has noted, "[i]f courts adopted this rule, it would subject anyone who is the subject of a custodial arrest, even for a traffic violation, to a preapproved foray into a virtual warehouse of their most intimate communications and photographs without probable cause." (Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, *supra*, 50 Santa Clara L. Rev. at p. 211.) United States Supreme Court authority does not compel this overly permissive rule, and I cannot agree to its adoption.

WERDEGAR, J.

I CONCUR:

MORENO, J.

OPPOSITION BRIEF

RECORD
AND
BRIEFS

No. 13-132

Supreme Court, U.S.
FILED
SEP 27 2013
OFFICE OF THE CLERK

In the Supreme Court of the United States

DAVID LEON RILEY, *Petitioner,*

v.

STATE OF CALIFORNIA, *Respondent.*

ON PETITION FOR A WRIT OF CERTIORARI TO THE CALIFORNIA COURT OF APPEAL, FOURTH DISTRICT

BRIEF IN OPPOSITION

KAMALA D. HARRIS
Attorney General of California
DANE R. GILLETTE
Chief Assistant Attorney General
JULIE L. GARLAND
Senior Assistant Attorney General
DONALD E. DE NICOLA
Deputy Solicitor General
A. NATASHA CORTINA
Supervising Deputy Attorney General
CHRISTINE LEVINGSTON BERGMAN*
Deputy Attorney General
110 West A Street, Suite 1100
San Diego, CA 92101
P.O. Box 85266
San Diego, CA 92186-5266
Telephone: (619) 645-2247
Fax: (619) 645-2271
Christine.Bergman@doj.ca.gov
**Counsel of Record*
Counsel for Respondent

Library of Congress
Law Library

QUESTION PRESENTED

After petitioner's lawful arrest for possession of loaded firearms, officers twice examined the contents of his cell phone, on his person at the time of his arrest, for evidence linking him to the firearms. The first examination, a cursory one of text entries, occurred at the scene of the arrest; the second, which included viewing photographs and videos, occurred a couple of hours later at the police station.

The question presented is:

Whether the officers' searches of the cell phone seized incident to petitioner's arrest were lawful under the Fourth Amendment.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

STATEMENT OF THE CASE 1

REASONS CERTIORARI SHOULD BE DENIED 6

I. The California Courts' Decision Comports With This Court's Fourth Amendment Precedents 6

II. Granting Certiorari Will Not Affect The Result, As Any Error In Admitting The Cell Phone Evidence Was Harmless Anyway 10

III. This Case Is A Poor Vehicle For Certiorari 11

CONCLUSION 14

TABLE OF AUTHORITIES

Page

CASES

Abel v. *United States*
362 U.S. 217 (1960) 8
Arizona v. *Fulminante*
499 U.S. 279 (1991) 10
City of Ontario, Cal. v. *Quon*
560 U.S. 746, 130 S.Ct. 2619 (2010) 13
Commonwealth v. *Berry*
979 N.E.2d 218 (Mass. 2012) 13
Commonwealth v. *Phifer*
979 N.E.2d 210 (Mass. 2012) 13
Hawkins v. *State*
723 S.E.2d 924 (Ga. 2012) 13
Maryland v. *King*
133 S.Ct. 1958 (2013) 9, 10
People v. *Diaz*
51 Cal.4th 84, 244 P.3d 501 (2011) 3, 4, 5, 6
People v. *Riley*
2013 WL 475242 6
Smallwood v. *State*
113 So.3d 724 (Fla. 2013) 13
State v. *Smith*
920 N.E.2d 949 (Ohio 2009), cert. denied,
131 S.Ct. 102 (2010) 13
Thornton v. *United States*
541 U.S. 615 (2004) 7
United States v. *Chadwick*
433 U.S. 1 (1977) 4, 6, 9
United States v. *Edwards*
415 U.S. 800 (1974) ..... 3 *et passim*

TABLE OF AUTHORITIES
(continued)

Page

United States v. *Finley*
477 F.3d 250 (5th Cir. 2007), cert. denied,
549 U.S. 1353 (2007) 13
United States v. *Flores-Lopez*
670 F.3d 803 (7th Cir. 2012) 13
United States v. *Murphy*
552 F.3d 405 (4th Cir. 2009), cert. denied,
129 S.Ct. 2016 (2009) 13
United States v. *Robinson*
414 U.S. 218 (1973) ..... 3 *et passim*
United States v. *Wurie*
2013 WL 2129119 13

CONSTITUTIONAL PROVISIONS

United States Constitution
Fourth Amendment ..... 5 *et passim*

STATEMENT OF THE CASE

Petitioner Riley is a member of a Blood gang called "Lincoln Park." On August 2, 2009, he and two fellow gang members armed themselves with handguns and parked petitioner's red Oldsmobile in San Diego's Skyline neighborhood, claimed by the rival Crips gang. When a Crips gang member drove by, petitioner and his cohorts fired several shots at him, causing him to crash. Petitioner and his cohorts drove off, and then hid petitioner's red Oldsmobile under a car cover a few miles away.

About three weeks later, San Diego police officers stopped petitioner, driving a different car, because the car's registration tags were expired. After discovering that petitioner was also driving with a suspended driver's license, the officers impounded the car and conducted an inventory search pursuant to standard police procedures. They found, hidden in the engine compartment, two loaded firearms. The officers arrested petitioner for carrying the concealed and loaded firearms.

In a search of petitioner at the arrest scene, one of the officers observed that he was wearing and possessed certain items indicating Lincoln Park gang membership: a green bandana in his pocket, and a keychain with a small pair of Converse red and green tennis shoes. The officer cursorily examined petitioner's cell phone[1], seized from his person at the time of arrest, and saw that all of the entries starting with a "k" were preceded by a "c." For Blood gang

---

[1] Petitioner asserts that his cell phone was a "Samsung Instinct M800 'smartphone'." See Pet. At 2. However, the record does not specify the type of cell phone found on petitioner.

members, such nomenclature is used to signify "Crip Killer."

At the police station about two hours later, a gang detective, aware that gang members often take pictures or videos of themselves with firearms, looked through petitioner's cell phone again. Looking for further evidence connecting petitioner to the firearms discovered in the car, the detective instead found some video clips of young men engaged in street boxing, a common gang initiation. In the video clips, the detective could hear petitioner saying, "Get brackin', Blood," and "Get him blood. Brack and Blood on Lincoln." In addition, petitioner's red Oldsmobile was visible in one of the videos. The detective also found on the cell phone photographs depicting petitioner and others making gang signs, including the hand sign for the letter "L."

Later, the police learned that petitioner's cell phone records—obtained through means unchallenged in this case—showed that his phone had been used near the location of, and around the same time as the August 2nd shooting. Those records also showed that the phone had been used about a half hour later near the location where the police in the meantime had found petitioner's Oldsmobile. Finally, the two handguns found in petitioner's engine compartment matched the guns used in the drive-by shooting.

The State charged petitioner with shooting at an occupied vehicle, attempted murder, and assault with a semiautomatic firearm.[2] The State further alleged, for sentence-enhancing purposes, that the

---

[2] Petitioner was separately charged with carrying a concealed firearm in a vehicle, carrying a loaded firearm, and receiving stolen property. He pled guilty to these charges and was sentenced to four years in state prison.

charged offenses had been gang-related and had involved the use of firearms.

Prior to his trial, petitioner moved to suppress the evidence found on his cell phone as invalid searches incident to arrest. After an evidentiary hearing, the trial judge denied the motion.

The judge ruled that, because the cell phone was on petitioner's person at the time of his arrest, the police were entitled to conduct a warrantless "search incident to arrest" under *United States* v. *Robinson*, 414 U.S. 218 (1973), and *United States* v. *Edwards*, 415 U.S. 800 (1974). The judge further noted that the detective had testified that, in his experience, gang members take photographs of themselves and their crimes, and that the detective had expected to find such photographs on petitioner's cell phone. As the judge explained, this established that the searches of petitioner's cell phone were conducted for investigative purposes relating to the crime for which petitioner had been arrested. The trial judge added that her ruling comported with the analysis endorsed by the California Court of Appeal in *People* v. *Diaz*, a case pending at that time for further review before the California Supreme Court.

Petitioner's first trial ended with a deadlocked jury. By the time of his re-trial, the California Supreme Court had decided *People* v. *Diaz*, 51 Cal.4th 84, 93, 244 P.3d 501 (2011). There the state supreme court held that the search of the text-message folder of Diaz's cell phone was a valid search incident to a custodial arrest. *Id.* at 502.[3] The state supreme court explained that the question was

---

[3] Two of the seven state supreme justices dissented on the ground that cell phones are qualitatively different than other items that may be found on an arrestee's person and are therefore entitled to greater protection.

controlled by this Court's decisions in *United States* v. *Robinson*, 414 U.S. 218, *United States* v. *Edwards*, 415 U.S. 800, and *United States* v. *Chadwick*, 433 U.S. 1 (1977):

> Under these decisions, the key question in this case is whether defendant's cell phone was "personal property . . . immediately associated with [his] person" (*Chadwick*, *supra*, 433 U.S. at p. 15) like the cigarette package in *Robinson* and the clothes in *Edwards*. If it was, then the delayed warrantless search was a valid search incident to defendant's lawful custodial arrest. If it was not, then the search, because it was "'remote in time [and] place from the arrest,'" "cannot be justified as incident to that arrest" unless an "exigency exist[ed]." [Footnote omitted.] (*Chadwick*, *supra*, at p. 15.)

Id. at 505.

Applying these precedents, the California Supreme Court determined that Diaz's cell phone was an item "immediately associated with the person of the arrestee" because the cell phone was an item of personal property on his person at the time of his lawful arrest and during the administrative processing at the police station. *People* v. *Diaz*, *supra*, 244 P.3d at 505-06. Accordingly, the state court concluded, petitioner's cell phone was properly subject to a warrantless station-house search. *Id.* at 511.

Before petitioner's second trial, the trial judge revisited her earlier rulings. The judge concluded that *Diaz* supported the ruling that the searches of the cell phone had been lawful incident to petitioner's arrest. So the judge again ruled the cell phone evidence admissible.

In addition to the evidence of petitioner's possession of the same guns used in the shooting, his cell phone records, and items on his person indicating a connection with a street gang, the jury at petitioner's re-trial heard recordings of several jailhouse calls made by petitioner a few days after his arrest, offered as incriminating himself in the shooting. In one, petitioner asked an unidentified woman "what exactly did my charges say?" After she said there were "gun charges," he asked, "But did it have—did it have any shooting stuff? It just had gun charges[,] right?" The woman told petitioner that it only had gun charges and a charge of driving without a license. Petitioner asked, "No type of shooting or any . . ." She said that it had some other "stuff" but that she did not know what it meant. Petitioner said, "it would say like attempted something or something like that."

In another phone call a couple of days later, petitioner said, "like no way that that shit, it's gonna come back to me like no matter what, the ballistics, it's gonna show . . ." In a different phone call, petitioner talked about getting bailed out because he knew what was going to "hit eventually." During some of the recorded telephone calls, further, petitioner used terminology that was common with gang members.

The jury found petitioner guilty as charged. The judge sentenced him to 15 years to life in state prison.

Petitioner appealed, challenging, among other things the trial judge's ruling on the suppression motion. In an unpublished decision, the California Court of Appeal affirmed the judgment in its entirety. The court of appeal concluded that "*Diaz* controls the present case" and held that the searches of the cell phone were lawful under the Fourth

Amendment as a searches incident petitioner's arrest because the cell phone "was 'immediately associated' with his 'person' when he was stopped." *People* v. *Riley*, 2013 WL 475242.

The California Supreme Court denied petitioner's petition for review without comment or citation.

REASONS CERTIORARI SHOULD BE DENIED

I. The California Court's Decision Comports With This Court's Fourth Amendment Precedents

This case involves a straightforward application of bedrock Fourth Amendment principles that have long governed the search of the person of the arrestee, notwithstanding the modern context involving a cell phone. The California courts in this case correctly applied this Court's precedents in concluding that the warrantless searches of petitioner's cell phone, on his person at the time of his arrest, was lawful.

Here, in upholding the searches of petitioner's cell phone, the California Court of Appeal was bound by the California Supreme Court's decision in *People* v. *Diaz*, which in turn was controlled by this Court's decisions in *United States* v. *Robinson*, 414 U.S. 218, *United States* v. *Edwards*, 415 U.S. 800, and *United States* v. *Chadwick*, 433 U.S. 1. Together, this Court's precedent stands for the principle that, while the Fourth Amendment prohibits the warrantless delayed search of items that merely had been "within the arrestee's immediate control," the search-incident-to-arrest exception to the search warrant requirement permits a delayed warrantless search of the person of the arrestee and of the personal property "immediately associated with the person of

the arrestee." In applying that principle, the California Court of Appeal correctly found that petitioner's cell phone was an item "immediately associated with the person of the arrestee," because the cell phone was an item of personal property on petitioner's person at the time of his lawful arrest. Accordingly, the California Court of Appeal correctly concluded that petitioner's cell phone was properly subject to the warrantless searches incident to lawful arrest.

In *Robinson*, 414 U.S. 218, the defendant was lawfully arrested and, upon his arrest, the arresting officer searched the defendant's pocket, extracted a cigarette package, and found heroin inside the package. *Id.* at 220-23. This Court upheld the search as a valid search incident to arrest. Id. at 236. It explained that, incident to a lawful custodial arrest, an officer has the authority to conduct "a full search of the person [of the arrestee]." *Id.* at 235. This authority, the Court explained, does not depend on whether the officer has reason to believe the arrestee has on his person either evidence or a weapon. Rather, it is the fact of arrest alone that justifies the search.

> A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a "reasonable" search under that Amendment.

Id.; see *Thornton* v. *United States*, 541 U.S. 615, 631-32 (2004) (Scalia, J., concurring). Thus, under

Robinson, a full search of the person of the arrestee is justified by virtue of the lawful arrest.

One year later, in *United States* v. *Edwards*, 415 U.S. 800, this Court once again addressed the lawful scope of the search of an arrestee and recognized that a valid search incident to arrest need not always be contemporaneous with the arrest. In *Edwards*, the defendant was lawfully arrested late one night for attempting to break into a post office. *Id.* at 801. He was transported to jail and placed in a cell. *Id.* Ten hours later, police had the defendant change into new clothing, holding on to his old clothing as evidence because they believed it might contain paint chips from the window through which he had tried to enter the post office. *Id.* at 801-02.

This Court upheld the warrantless search and seizure of the defendant's clothing under the search-incident-to-arrest exception to the search warrant requirement. *United States* v. *Edwards*, 415 U.S. at 802-09. The Court explained that "searches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention." *Id.* at 803. The Court noted that this question had been settled by its prior decision in *Abel* v. *United States*, 362 U.S. 217 (1960). *Id.* at 803. The Court explained:

> [O]nce the accused is lawfully arrested and is in custody, the effects in his possession at the place of detention that were subject to search at the time and place of his arrest may lawfully be searched and seized without a warrant even though a substantial period of time has elapsed between the arrest and subsequent administrative processing, on the one hand, and the taking of the property for use as evidence, on the other.

Edwards at 807. Thus, under *Edwards*, the person of the arrestee and the property in his possession at the detention facility are properly subject to a warrantless station-house search.

Subsequently, in *United States* v. *Chadwick*, 433 U.S. 1, this Court revisited the exception to the requirement that a search incident to arrest be contemporaneous with the arrest and specified that the exception applied to the person of the arrestee and personal property "immediately associated with the person of the arrestee." Applying this principle, the Court invalidated a search where officers had seized a 200-pound, double-locked footlocker during the defendant's arrest and then had searched the footlocker without a warrant an hour and a half later. *Id.* at 4-5. But the Court distinguished such searches of possessions within the arrestee's control from searches of the arrestee's person and items "immediately associated with the person of the arrestee. Although distinguishing it, this Court thus reaffirmed the search of an arrestee's person under *Edwards*. *Id.* at 16 n.10. Most recently, in *Maryland* v. *King*, 133 S.Ct. 1958 (2013), this Court re-affirmed that the "constitutionality of a search incident to an arrest does not depend on whether there is any indication that the person arrested possesses weapons or evidence." *Id.* at 1971 (citation omitted). In doing so, it reaffirmed the core holding of *Robinson* by reiterating that "[t]he fact of a lawful arrest, standing alone, authorizes a search." *Id.* at 1971 (citation omitted). In *King*, this Court upheld the warrantless DNA testing of persons arrested for serious crimes, relying on the government's important interest in identifying an arrestee, including verifying his name and determining his criminal history, and the arrestee's diminished

expectation of privacy in his person. *King* at 1971, 1978.

These precedents validate the warrantless searches of petitioner's cell phone. It was an item of personal property on his person at the time of his lawful arrest. Like the clothing taken from the defendant in *Edwards*, petitioner's cell phone was an item "immediately associated with the person of the arrestee."

II. Granting Certiorari Will Not Affect The Result, As Any Error In Admitting The Cell Phone Evidence Was Harmless Anyway.

Further, the result in this case would stand regardless of whether or how this Court might resolve the question presented in the petition. Even if the evidence taken from petitioner's cell phone had been excluded, he still would have been found guilty of the charged offenses because there was ample independent evidence supporting the guilty verdict and sentence-enhancement findings. That is, the alleged error was harmless beyond a reasonable doubt. See *Arizona* v. *Fulminante*, 499 U.S. 279, 306-07 (1991).

Strong evidence, other than that found in the cell phone, linked petitioner to the drive-by shooting. The day after the shooting, San Diego police officers found the hidden red Oldsmobile. The car was registered to petitioner and a traffic citation in petitioner's name was inside the car. Petitioner's girlfriend, moreover, lived down the street from the scene of the shooting. In addition, unchallenged cell phone records confirmed that petitioner's cell phone had been used in the vicinity of the shooting on the date and near the time of the shooting, and that it then used about a half hour later where the

Oldsmobile was parked. Even more, ballistics tests revealed that the two firearms found in engine compartment of petitioner's car were used during the drive-by shooting. Petitioner's DNA was found on one of these guns. Finally, petitioner's recorded jailhouse calls confirmed his involvement in the shooting.

The information the police retrieved from petitioner's cell phone was merely trivial and surplus evidence showing petitioner's gang involvement and thus proving the sentence-enhancing special allegation. A gang expert, with approximately 12 prior contacts with petitioner and other Lincoln Park gang members, testified at trial that petitioner was a documented Lincoln Park gang member. The expert further attested that he had seen petitioner, making gang signs, depicted in photographs (not those recovered from the cell phone) with known Lincoln Park gang members. Petitioner also had a gang moniker, "Dave Bo"; and the green bandana he was wearing at the time of his arrest further evidenced his Lincoln Park gang membership. During his recorded jailhouse calls, moreover, petitioner used terminology commonly used by gang members.

Thus, any error in admitting the photographs and videos retrieved from the cell phone was harmless beyond a reasonable doubt. Accordingly, resolution of the Question Presented would be an abstract undertaking that would not affect the judgment.

III. This Case Is A Poor Vehicle For Certiorari

Last, this case is, for other reasons, a poor candidate for certiorari.

1. First, the certiorari petition seeks to present multiple complicated issues for this Court to resolve. Petitioner asks this Court to consider whether various kinds of digital content produce different privacy concerns than others. Petitioner also asks this Court to consider the two searches of his cell phone as two separate issues. Pet. at 20.

2. Second, the record does not clearly support petitioner's suggestion that the search involved "a range of different types of digital content stored on cell phones" that are more characteristic of a modern smart phone. See Pet. at 20. The record is vague regarding what exactly the officers did with the cell phone, and how they accessed the information on the cell phone. The officers' testimony merely establishes the first search entailed looking at text entries, and the second search involved looking at photographs and videos. There is no evidence concerning whether the officers accessed any information on the cell phone such as appointment calendars, e-mail correspondence, internet-related activity, or applications—features commonly associated with a smart phone. Based on the record, the search involved no intrusion greater than the viewing of the photographs, video and text entries on the cell phone. Therefore, the record does not support petitioner's portrayal of an unfettered search through a wide range of information disclosing petitioner's personal and private affairs.

3. Respondent acknowledges that there is a growing conflict concerning whether the Fourth Amendment permits law enforcement officers to search the contents of a cell phone incident to arrest as argued by petitioner. (Pet. at 7-13.) But, as explained above, that does not mean that granting certiorari would be warranted or necessary or useful in this particular case.

A more likely candidate for resolving the conflict may be found elsewhere. Most significant, the First Circuit in *United States* v. *Wurie*, 2013 WL 2129119 recently joined Ohio (*State* v. *Smith*, 920 N.E.2d 949, 952-955 (Ohio 2009), cert. denied, 131 S.Ct. 102 (2010)), and Florida (*Smallwood* v. *State*, 113 So.3d 724, 734-738 (Fla. 2013)), in holding that such a cell phone search violated the Fourth Amendment. *Wurie* created a split with the Fourth, Fifth, and Seventh Circuits, and also conflicts with decisions of the supreme courts of Massachusetts and Georgia—and California. See *United States* v. *Finley*, 477 F.3d 250 (5th Cir. 2007), cert. denied, 549 U.S. 1353 (2007); *United States* v. *Murphy*, 552 F.3d 405 (4th Cir. 2009), cert. denied, 129 S.Ct. 2016 (2009); *United States* v. *Flores-Lopez*, 670 F.3d 803 (7th Cir. 2012); *Hawkins* v. *State*, 723 S.E.2d 924, 925-936 (Ga. 2012); *Commonwealth* v. *Phifer*, 979 N.E.2d 210 (Mass. 2012); *Commonwealth* v. *Berry*, 979 N.E.2d 218 (Mass. 2012). And the United States government has filed a petition for writ of certiorari in *Wurie*, No. 13-212 (filed August 15, 2013). Further, as *Wurie* appears to involve a more basic kind of cell phone, certiorari review in that case would allow the Court to approach the issue in a measured way, first in the context of a settled technology—rather than in the still rapidly changing technological context of "smart phones." See *City of Ontario, Cal.* v. *Quon*, 560 U.S. 746, 130 S.Ct. 2619, 2629 (2010). Moreover, the record in *Wurie* might well be clear—in a way the record in this case is not—about exactly how and where the police accessed the challenged evidence from the phone. Those circumstances would need to be understood in order to properly gauge the defendant's reasonable expectation of privacy in resolving the Fourth Amendment issue.

CONCLUSION

The petition for writ of certiorari should be denied.

Respectfully submitted

KAMALA D. HARRIS
Attorney General of California
DANE R. GILLETTE
Chief Assistant Attorney General
JULIE L. GARLAND
Senior Assistant Attorney General
DONALD E. DE NICOLA
Deputy Solicitor General
A. NATASHA CORTINA
Supervising Deputy Attorney General
CHRISTINE LEVINGSTON BERGMAN*
Deputy Attorney General
**Counsel of Record*
Counsel for Respondent

September 26, 2013

CMLB:lb
SD2013806433
80821444.doc

REPLY BRIEF

Supreme Court, U.S.
FILED
OCT 16 2013
OFFICE OF THE CLERK

RECORD
AND
BRIEFS

No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Petition for a Writ of Certiorari
to the California Court of Appeal, Fourth District

REPLY BRIEF FOR PETITIONER

Patrick Morgan Ford
LAW OFFICE OF PATRICK
MORGAN FORD
1901 First Avenue,
Suite 400
San Diego, CA 92101

Kevin K. Russell
GOLDSTEIN &
RUSSELL, P.C.
5225 Wisconsin Ave., NW
Suite 404
Washington, DC 20036

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@law.stanford.edu

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

REPLY BRIEF FOR PETITIONER 1

I. This Case Is An Excellent Vehicle For Considering The Question Presented 1

II. The Search Here Violated The Fourth Amendment 7

CONCLUSION 8

TABLE OF AUTHORITIES

Cases

Bullcoming v. New Mexico, 131 S. Ct. 2705 3

Lily v. Virginia, 527 U.S. 116 (1999) 3

Maryland v. King, 133 S. Ct. 1958 (2013) 7

People v. Diaz, 244 P.3d 501 (Cal. 2011), *cert denied*, 132 S. Ct. 94 (2011) 7

United States v. Jones, 132 S. Ct. 945 (2012) 6

United States v. Wurie, No. 13-212 ..... 1, 4, 5, 6

Wong Sun v. United States, 371 U.S. 471 (1963) 3

Constitutional Provision

U.S. Const., amend. IV 1, 5, 7, 8

REPLY BRIEF FOR PETITIONER

The State "acknowledges that there is a growing conflict concerning whether the Fourth Amendment permits law enforcement officers to search the contents of a cell phone incident to arrest." BIO 12. The issue also arises on a daily basis across the country. *See* Pet. 14. Hence, the importance of resolving the conflict this Term is evident – as the *amici* in this case and the Solicitor General in *United States v. Wurie*, No. 13-212, also recognize. That leaves the State to argue in its brief in opposition only (1) that this case is an unsuitable vehicle for resolving the conflict; and (2) that the holding below is correct on the merits. Neither of these arguments, however, provides any reason to deny review – or to grant certiorari in *Wurie* in lieu of this case.

I. This Case Is An Excellent Vehicle For Considering The Question Presented.

None of the State's quibbles about this case as a vehicle for resolving the question presented withstands scrutiny.

1. The State first asserts without argument that the fact that this case involved two separate searches – one at the scene of the arrest and a second by a different officer several hours later at the police station – makes this case a poor vehicle. BIO 12. But as petitioner has already explained, the two searches in this case actually make this case an ideal vehicle for supplying comprehensive guidance on how the search-incident-to-arrest doctrine applies to cell phones. In particular, the two searches in this case would allow this Court to address the crosscurrents in its doctrine concerning how close in time and space

a search must be to an arrest to be properly incident to that arrest. *See* Pet. 20-21.

2. The State next contends that the record is "vague regarding what exactly the officers did with the cell phone, and how they accessed the information on the cell phone." BIO 12. But the record is settled on the facts that matter. There is no doubt that the arresting officer searched through the phone's text messages folder at the scene of the arrest. Pet. 3; BIO 12. It also is clear that the detective specializing in gang investigations later searched through "a lot of stuff" on the phone at the police station while "looking for evidence." Pet. 3 (quoting detective's testimony at Tr. 176, 193). At a minimum, that second search involved the phone's folders containing photos and videos. *Id.*; BIO 12. These undisputed facts are more than enough to show that this case involves a wide-ranging and intrusive examination of the digital contents of a smartphone – exactly the kind of search that, for all of the reasons petitioner and *amici* have explained, provides the best setting for considering the question presented.[1]

3. Although the State never argued below that any Fourth Amendment violation was harmless, it

---

[1] The State asserts that "the record does not specify the type of cell phone found on petitioner." BIO 1 n.1. But given that the State itself provided petitioner during discovery with a document entitled "phone examination report properties" noting that the phone was a "Samsung" "SPH-M800 Instinct," it is impossible to dispute – and the State does not actually do so – that petitioner has accurately described the smartphone at issue. *See* Pet. 2.

now advances such a contention for the first time. BIO 10-11. This contention provides no impediment to review because this Court's practice at the merits stage when a state contends that a constitutional criminal procedure error was harmless is to resolve the constitutional claim and then to "allow[] state courts initially to assess the effect of erroneously admitted evidence in light of substantive state criminal law." *Lilly v. Virginia*, 527 U.S. 116, 139 (1999); *see also, e.g.*, *Bullcoming v. New Mexico*, 131 S. Ct. 2705, 2719 n.11 (2011).

At any rate, the State's harmless-error argument is unpersuasive. The State's case was entirely circumstantial and petitioner's first trial (which was based on the same evidence as the second trial) ended in a hung jury, *see* Pet. 4, so every marginal piece of evidence the State offered was critical. And the text entries, photos, and videos gleaned from petitioner's phone were especially critical. The State thus stressed the photos and videos in its closing argument as pieces of the evidentiary "puzzle" supposedly linking petitioner to the shootings. Tr. 1161. Indeed, that evidence is what caused petitioner first to become a suspect in this case and also led to other evidence that might be considered upon full briefing on remand to be fruit of the poisonous tree. Pet. 3; BIO 1-2; *see generally Wong Sun v. United States*, 371 U.S. 471, 488 (1963) (fruit of poisonous tree doctrine).

What is more, the prosecution relied heavily on the photos and videos at trial in its effort to prove that petitioner committed the crimes here for the benefit of a gang. The gang aggravating factor enhanced petitioner's sentence from a maximum of

seven years to a minimum of fifteen, thus making the evidence highly consequential for that reason alone. *See* Pet. 5. Moreover, purported gang evidence naturally has a powerful effect on a jury's broader deliberations, particularly in a circumstantial case.

4. Finally, the State suggests that *Wurie* is a better candidate for certiorari than this case because *Wurie* involved "a more basic kind of cell phone." BIO 13. But, as several *amici* in this case have already explained, just the opposite is true. This case is the superior one because it involves the smartphone technology most prevalent today (and that will be the industry standard for years to come), while *Wurie* involves a virtually defunct "flip phone" device. *See* Br. for Center for Democracy & Technology and Electronic Frontier Foundation at 11-13; Br. for NACDL 11-12. It should go without saying that this Court's resources are better spent deciding a case concerning current reality than one involving a relic of the past.

Even if this Court wishes for some reason to pass judgment on the search of the old-fashioned flip phone in *Wurie*, it should also grant plenary review in this case. When it sought en banc review in *Wurie*, the United States acknowledged that a ruling in that case would not necessarily determine the constitutionality of the search of a modern smartphone. Specifically, the government conceded that "certain cell-phone searches might be so intrusive as to be unreasonable – just as a thorough search of a personal diary might be unreasonable in a particular case." U.S. Pet. for Rehearing En Banc at 11, *United States v. Wurie*, No. 11-1792 (1st Cir. July 16, 2013). This is because "[i]n cases involving more

intrusive searches of computer-like phones, the core Fourth Amendment requirement of reasonableness protects against unwarranted invasions of privacy, as the Supreme Court has repeatedly stated." *Id.* at 6-7. Yet the government asserted that "[t]o the extent that some cell phones may implicate more serious concerns than traditional containers, those concerns are not present in [*Wurie*], which involved a brief examination of the call log of a flip phone." *Id.* at 6.[2]

This case involves the kind of "intrusive" search of a "computer-like" phone that the government has stressed did *not* occur in *Wurie*. And petitioner concurs with the government that these distinctions may well matter. *See* Pet. 25-28. In contrast to a flip phone, the immense storage capacity and multimedia components of a smartphone render it the digital equivalent of an entire house full of personal diaries, letters, photo albums, and DVD's. *See* Br. for Center for Democracy and Technology and Electronic Frontier Foundation at 3-13; Br. for NACDL Br. 2-19. These practical capabilities may be relevant not only to any overall "reasonableness" inquiry, *see United States v. Jones*, 132 S. Ct. 945, 955-57 (2012) (Sotomayor, J., concurring); *id.* at 963 (Alito, J.,

---

[2] The government's position in this Court is less clear. At one point, the government states – as in the First Circuit – that "if officers may be found to act unreasonably in violation of the Fourth Amendment by reading highly personal papers found during a search of a person incident to arrest, similar principles could apply to cell-phone searches." Pet. for Cert. in *Wurie* 17. At other points, the government seeks a "bright-line rule" authorizing any search of any kind of cell phone incident to arrest. *Id.* at 11, 16.

concurring in the judgment), but also to the question whether the searches at issue implicate the Framers' intent to prohibit the use of "general warrants," Br. for Constitutional Accountability Center at 5-20. Thus, regardless of what this Court does with the *Wurie* petition, it should grant certiorari here to ensure that it is able to deliver a ruling on the question presented that gives genuine guidance for future cases.[3]

---

[3] In *Wurie* (Pet. for Cert. 26 & n.4), the Solicitor General suggests that *Wurie* is different than this case insofar as that case raises the alternative argument that "a particular search is permissible where it is reasonable to believe that evidence of the offense of arrest might be found on the phone . . . or where the search is reasonably targeted to information likely to shed light on an arrestee's identity" (internal citations and quotation marks omitted). There is nothing to this suggestion. The prosecution in either case may, if it chooses, advance such a legal argument in this Court; the Solicitor General could advance it as *amicus* in this case as well. And in either case, this Court, if it agreed with the argument, could say so in an opinion and either apply the argument to the facts of the case or remand for such an application.

If anything, the Solicitor General's professed interest in arguing in the alternative that some sort of "reasonable belief" test applies in this context underscores the need to grant certiorari in a case involving a smartphone. However such a theory might play out with respect to a simple flip phone, the vast amount of personal information stored on a smartphone raises the possibility that any exception allowing warrantless cell-phone searches based on a reasonable expectation of finding relevant evidence inside would entirely swallow a general rule prohibiting such searches.

II. The Search Here Violated The Fourth Amendment.

None of the State's arguments on the merits affords any reason to deny review.

Echoing the California Supreme Court's decision in *People v. Diaz*, 244 P.3d 501 (Cal. 2011), *cert denied*, 132 S. Ct. 94 (2011) (Pet. App. 25a-65a), the State argues that the searches of petitioner's smartphone comported with the Fourth Amendment because decisions that this Court rendered in the 1970's categorically allow the police to search "an[y] item of personal property on [an arrestee's] person at the time of his lawful arrest." BIO 10. Petitioner has already explained how this argument overreads this Court's precedent and ignores fundamental differences between the digital contents of smartphones and the ordinary physical contents of traditional containers. *See* Pet. 21-28. The State also contends that this Court's recent decision in *Maryland v. King*, 133 S. Ct. 1958 (2013), supports its categorical view of the search-incident-to-arrest doctrine. BIO 9-10. If anything, however, *King* bolsters petitioner's argument. *King* makes clear that "the ultimate measure of the constitutionality" of a search incident to arrest "is reasonableness," which includes an assessment of the "scope and manner of execution" of the search. 133 S. Ct. at 1969-70. That sort of textured and item-specific inquiry is exactly what petitioner and *amici* have explained may be decisive here. Pet. 25-28; Br. for Center for Democracy and Technology and Electronic Frontier Foundation at 9-11.

In any event, the conflict in the lower courts over the question presented renders certiorari essential

regardless of what the Constitution dictates here. Whatever this Court ultimately decides the Fourth Amendment permits police officers to do when seizing smartphones incident to arrest, the important point is that officers (and citizens, lawyers, and courts) need to know now what is allowed and what is not. This Court should grant review in this case to deliver that comprehensive guidance.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Patrick Morgan Ford
LAW OFFICE OF PATRICK MORGAN FORD
1901 First Avenue, Suite 400
San Diego, CA 92101

Kevin K. Russell
GOLDSTEIN & RUSSELL, P.C.
5225 Wisconsin Ave., NW
Suite 404
Washington, DC 20036

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

October 16, 2013

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

AUG 30 2013

No. 13-132

In the Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Petition for a Writ of Certiorari to the California Court of Appeal, Fourth District

BRIEF OF CENTER FOR DEMOCRACY & TECHNOLOGY AND ELECTRONIC FRONTIER FOUNDATION AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

ANDREW J. PINCUS
Counsel of Record
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

Library of Congress
Law Library

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 3

A. Smartphone Technology Fundamentally Changes The Quantity And Types Of Information That A Person Can Carry 3

B. The Changes Resulting From Smartphone Technology Are Highly Relevant To Application Of The Search-Incident-To-Arrest Doctrine 9

C. This Court Should Consider The Search-Incident-To-Arrest Issue In The Context Of A Search Implicating The New Capabilities Of Today's Smartphones 11

CONCLUSION 14

TABLE OF AUTHORITIES

Page(s)

CASES

Chimel v. *California*, 395 U.S. 752 (1969) 9

City of Ontario v. *Quon*,
130 S. Ct. 2619 (2010) 1, 2, 10

Commonwealth v. *Phifer*,
979 N.E.2d 210 (Mass. 2012) 12

Kyllo v. *United States*, 533 U.S. 27 (2001) 2

Smallwood v. *State*,
113 So.3d 724 (Fla. 2013) 5, 7

State v. *Smith*,
920 N.E.2d 949 (Ohio 2009), cert. denied,
131 S. Ct. 102 (2010) 7

United States v. *Edwards*,
415 U.S. 800 (1974) 10

United States v. *Jones*,
132 S. Ct. 945 (2012) ..... *passim*

United States v. *Robinson*,
414 U.S. 218 (1973) 9

United States v. *Wurie*,
2013 WL 2129119 (1st Cir. May 17, 2013),
petition for cert. filed, No. 13-212 (U.S.
Aug. 15, 2013) 6, 7, 12

CONSTITUTION

U.S. Const. amend. IV 1, 2, 10, 11

TABLE OF AUTHORITIES—continued

Page(s)

MISCELLANEOUS

AT&T, *What is a smartphone?*, at http://www.att. com--/esupport/article. jsp?sid=KB101001&cv=821#fbid=ePYU9KGCdmS 4

Tim Bajarin, *Why Your Smartphone Will Be Your Next PC*, TIME Tech, Feb. 25, 2013, available at http://techland.time.com/2013/02/25/why-your-smartphone-will-be-your-next-pc/#ixzz2dIA7OWki 8

Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, Pew Research Center, Nov. 2012, available at http://www.pew-internet.org/~/media//Files/Reports/2012/PIP_CellActivities-_11.-25.pdf 4, 5, 6

Barb Dybwad, *4 Simple iPhone Apps for Creating and Editing Documents*, Entrepreneur, Oct. 31, 2012, available at http://www.entrepreneur.com/blog/224803 5

Michael Gorman, *Facebook's move to mobile powered by intensive internal training*, Engadget, Mar. 4, 2013, available at http://www.engadget.-com/2013/03/04/facebooks-move-to-mobile-powered-by-intensive-internal-training/ 7

John Granby, *Instant Messaging Using an iPhone*, Houston Chronicle, available at http://smallbusiness.chron.com/instant-messaging-using-iphone-68883.html 5

TABLE OF AUTHORITIES—continued

Page(s)

iTunes Preview, at https://itunes.apple.-com/us/genre/ios/id36?mt=8 6

Orin S. Kerr, *Foreward: Accounting for Technological Change*, 36 Harv. J.L.& Pub. Pol'y 403 (2013) 6

Orin Kerr, *Two Petitions on Searching Cell Phones Reach the Supreme Court*, The Volokh Conspiracy, Aug. 19, 2013, available at http://www.-volokh.com/2013/08/19/doj-files-cert-petition-in-wurie/ 13

Mary Kozelka, *The key to better health care may already be in your pocket ... and it's not your wallet*, NBC News, Jan. 24, 2013, available at http://rockcenter.nbcnews.-com/_news/2013/01/24/16677207-the-key-to-better-health-care-may-already-be-in-your-pocket-and-its-not-your-wallet?lite 5

Hugo Miller, *BlackBerry to Offer BBM Messaging App on Apple, Android Devices*, Bloomberg, May 14, 2013, available at http://www.bloom-berg.com/news-/2013-05-14/blackberry-to-offer-bbm-messaging-app-on-apple-android-devices.html 5

PC Magazine Encyclopedia, *Definition of: smartphone*, at http://www.pcmag.com /encyclopedia/term/51537/smartphone 4

Paul Ridden, *Casetop 'laptop' uses your smartphone as its brains*, Gizmag, May 7, 2013, available at http://www.gizmag. com /livi-design-casetop/27418/ 8

TABLE OF AUTHORITIES—continued

Page(s)

Aaron Smith, *Smartphone Ownership – 2013 Update*, Pew Research Center, June 2013, available at http://pewinternet.org/~/-media//Files/Reports/2013/PIP_Smart-phone_adoption_2013.pdf 4

Elizabeth Stawicki, *Need your medical records? There's an app for that*, MPRnews, May 1, 2013, available at http:// minnesota. publicradio. org/display/ web/2013/05/01/health/medical-records-application 5

INTEREST OF THE *AMICI CURIAE*

The Center for Democracy & Technology (CDT) is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing civil liberties issues raised by emerging technologies.

CDT and EFF have participated as *amici* in cases before this Court involving the application of the Fourth Amendment to new technologies, including *City of Ontario* v. *Quon*, 130 S. Ct. 2619 (2010), and *United States* v. *Jones*, 132 S. Ct. 945 (2012).[1]

[1] Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici* and their counsel made a monetary contribution to its preparation or submission. Counsel of record for all parties received notice at least 10 days prior to the due date of the intention of *amici* to file this brief. The parties' letters consenting to the filing of this brief have been filed with the Clerk's office.

SUMMARY OF ARGUMENT

The Court repeatedly has recognized the importance of carefully assessing the nature and effects of new technologies in determining whether a government search is "unreasonable" within the meaning of the Fourth Amendment. *United States* v. *Jones*, 132 S. Ct. 945 (2012); *City of Ontario* v. *Quon*, 130 S. Ct. 2619 (2010); *Kyllo* v. *United States*, 533 U.S. 27 (2001).

This case presents a question regarding the impact of new technology in a context familiar to most Americans: today's mobile telephones—known as "smartphones"—which can, and increasingly do, contain the equivalent of millions of physical pages of information, much of it highly personal. The particular issue is whether the search-incident-to-arrest exception to the requirement of a warrant and probable cause permits the government to review all of the information stored in a smartphone simply because an individual is carrying the phone when he or she is arrested.

The lower courts have reached conflicting conclusions regarding that question, with some courts taking account of the effect of new technology and other courts concluding that that effect is irrelevant under the Fourth Amendment. This Court's review is needed to resolve that clear disagreement and to make clear that here, as in *Jones* and *Kyllo*, the changes resulting from new technology impact significantly the reasonableness determination under the Fourth Amendment.

The Court should address that question in a case, such as this one, that involves some of the extensive capabilities of smartphones, the type of mo-

bile phone that is now used by the majority of Americans. The Solicitor General's petition presenting a question regarding the search-incident-to-arrest exception, *United States* v. *Wurie*, No. 13-212 (filed Aug. 15, 2013), involves an old-technology mobile phone used by a decreasing minority of Americans. The facts of that case accordingly do not illustrate the dramatic effect of today's technology, which is critically relevant to the Fourth Amendment's reasonableness inquiry.

The Court should therefore grant review in this case, which involves the more prevalent form of technology, to resolve the conflict among the lower courts regarding this important, frequently-arising issue.

ARGUMENT

A. Smartphone Technology Fundamentally Changes The Quantity And Types Of Information That A Person Can Carry.

Prior to the advent of digital technology, an individual could transport information only if the information was printed on paper, etched on vinyl, or recorded on film. That reality restricted the total amount of information that a person could carry. And it meant that individuals did not routinely have on their persons large amounts of personal information, particularly personal financial and medical information.

The first mobile telephones did not alter that state of affairs because they had only one function: enabling an individual to place and receive telephone calls. Subsequent iterations of these phones permitted the owner to create an electronic "contact list" of names and telephone numbers and to save the tele-

phone numbers called and the numbers from which calls were received.

Technological advances have moved far beyond these rudimentary features, however. According to a recent survey, a majority of American adults—56%—now own smartphones with much more expansive capabilities, and that percentage is almost certain to increase significantly in the next few years.[2] These devices combine the features of a mobile phone and those of a computer, with access to both the voice network and the Internet.[3] Typically, smartphones allow individuals to:

- Receive, store, and send emails with attached documents;[4]
- Conduct—and store—private text "conversations" with one or more particular individu-

---

[2] Aaron Smith, *Smartphone Ownership – 2013 Update*, Pew Research Center, June 2013, at 2, available at http://pewinternet.org/~/-media//Files/Reports/2013/PIP_Smartphone_adoption_2013.pdf. Because "ownership is particularly high among younger adults, especially those in their twenties and thirties" (*id.* at 3), the overall percentage will increase as more individuals enter that age cohort.

[3] See AT&T, *What is a smartphone?*, at http://www.att.com/esupport/article.jsp?sid=KB101001&cv=821#fbid=ePYU9KGCdmS; PC Magazine Encyclopedia, *Definition of: smartphone*, at http://www.pcmag.com/encyclopedia/term/51537/smartphone.

[4] Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, Pew Research Center, Nov. 2012, at 7, available at http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.-25.pdf.

als in writing using instant messaging and similar features;[5]

- Create and store personal documents;[6]
- Create and store personal photographs and videos;[7]
- Access the Internet (and retain a record of internet sites visited);[8]
- Create and store appointment calendars;[9]
- Conduct personal financial transactions and store financial information;[10] and
- Conduct medical tests and store medical information.[11]

---

[5] John Granby, *Instant Messaging Using an iPhone*, Houston Chronicle, available at http://smallbusiness.chron.com/instant-messaging-using-iphone-68883.html; Hugo Miller, *BlackBerry to Offer BBM Messaging App on Apple, Android Devices*, Bloomberg, May 14, 2013, available at http://www.bloomberg.com/news-/2013-05-14/blackberry-to-offer-bbm-messaging-app-on-apple-android-devices.html; see also Duggan & Rainie, *supra*, at 5.

[6] Barb Dybwad, *4 Simple iPhone Apps for Creating and Editing Documents*, Entrepreneur, Oct. 31, 2012, available at http://www.entrepreneur.com/blog/224803; see also http://www.-apple.com/apps/iwork/pages/.

[7] Duggan & Rainie, *supra*, at 4, 8.

[8] *Id.* at 6.

[9] *Smallwood* v. *State*, 113 So.3d 724, 729, 731-732 (Fla. 2013).

[10] Duggan & Rainie, *supra*, at 10.

[11] Elizabeth Stawicki, *Need your medical records? There's an app for that*, MPRnews, May 1, 2013, available at http://minnesota.publicradio.org/display/web/2013/05/01/health/medical-records-application; Mary Kozelka, *The key to better health care may already be in your pocket ... and it's not your*

With the dramatic growth of "applications" that can be loaded onto smartphones, these are only a few of literally thousands of different functions that these devices can perform, and only a few examples of the types of information that they can and do contain.[12]

Moreover, the amount of information that can be stored on a smartphone is extraordinary. A single phone can hold data equivalent to millions of pages of text.[13] That is "similar to the typical storage capacity of a home computer sold in 2004."[14]

As the Florida Supreme Court recently explained,

> Vast amounts of private, personal information can be stored and accessed in or through these small electronic devices, including not just phone numbers and call his-

---

wallet, NBC News, Jan. 24, 2013, available at http://rockcenter.nbcnews.-com/_news/2013/01/24/16677207-the-key-to-better-health-care-may-already-be-in-your-pocket-and-its-not-your-wallet?lite; Duggan & Rainie, *supra*, at 3.

[12] The "App Store," at which an iPhone user may obtain "Apps"—applications—that program the iPhone to perform a wide variety of functions, contains nearly 1 million different applications, many of which involve storage of personal information. See *iTunes Preview*, at https://itunes.apple.-com/us/genre/ios/id36?mt=8 (webpage listing iPhone apps).

[13] "Apple's iPhone 5 comes with up to sixty-four gigabytes of storage, which is enough to hold about 'four million pages of Microsoft Word documents.'" *United States* v. *Wurie*, 2013 WL 2129119, at *6 (1st Cir. May 17, 2013) (citation omitted), petition for cert. filed, No. 13-212 (U.S. Aug. 15, 2013). The memory capacity of most smartphones ranges from 16 to 64 gigabytes.

[14] Orin S. Kerr, *Foreward: Accounting for Technological Change*, 36 Harv. J.L.& Pub. Pol'y 403, 404 (2013), available at http://www.harvard-jlpp.com/wp-content/uploads/2013/04/-36_-2_403_Kerr.pdf.

> tory, but also photos, videos, bank records, medical information, daily planners, and even correspondence between individuals * * *. The most private and secret personal information and data is contained in or accessed through small portable electronic devices and, indeed, many people now store documents on their equipment that also operates as a phone that, twenty years ago, were stored and located only in home offices, in safes, or on home computers.

Smallwood v. *State*, 113 So. 3d 724, 731-732 (Fla. 2013); see also *United States* v. *Wurie*, 2013 WL 2129119, at *7 (1st Cir. May 17, 2013) ("information [stored in smartphones] is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records"), petition for cert. filed, No. 13-212 (U.S. Aug. 15, 2013); *State* v. *Smith*, 920 N.E.2d 949, 955 (Ohio 2009) (same), cert. denied, 131 S. Ct. 102 (2010).

Indeed, smartphone owners use these devices to replicate—and in some cases to replace entirely—the functions performed on personal computers. That is why companies such as Facebook are now focused on using smartphones as a platform for their services. See, *e.g.*, Michael Gorman, *Facebook's move to mobile powered by intensive internal training*, Engadget, Mar. 4, 2013, available at http://www.engadget.com/2013/03/04/facebooks-move-to-mobile-powered-by-intensive-internal-training/ ("Facebook's made no bones about the fact that its focus has shifted from a desktop web- to a mobile-focused company").

Some observers predict that a "new computing paradigm could emerge in which the smartphone actually becomes the center of our personal computing universe." Tim Bajarin, *Why Your Smartphone Will Be Your Next PC*, TIME Tech, Feb. 25, 2013, available at http://techland.time.com/2013/02/25/why-your-smartphone-will-be-your-next-pc/#ixzz2dIA7OWki. Because "the smartphone has all of [the user's] personal data, personal user interface and personal apps," the smartphone could simply be connected to a desktop monitor or a laptop computer with no permanent memory to enable the user to use a keyboard and larger screen; personal information would be stored only on the smartphone. *Ibid.*; see also Paul Ridden, *Casetop 'laptop' uses your smartphone as its brains*, Gizmag, May 7, 2013, available at http://www.gizmag.com/livi-design-casetop/27418/ (observing that "modern smartphones are just like mini computers that can be carried around in your pocket" and reviewing a new product that "uses a smartphone for its computing power" and as the source of the user's personal information).

Smartphone technology has thus produced an incredible change in the quantity and type of information that individuals routinely have in their immediate possession. Previously, no individual could carry, either on his or her person or in a container, even a small fraction of the information contained in today's smartphones. In physical form—paper documents, photographs, etc.—the information would be too bulky and too heavy to carry. Because of those physical limitations, moreover, no individual could routinely carry all of his or her personal financial or medical information.

Today, it is no exaggeration to state that an individual can, and often does, carry at all times the extremely personal information that formerly would have been stored in the individual's residence.

B. The Changes Resulting From Smartphone Technology Are Highly Relevant To Application Of The Search-Incident-To-Arrest Doctrine.

"In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." *Jones*, 132 S. Ct. at 963 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment). Thus, the amount of information that the government could obtain under the search-incident-to-arrest exception was circumscribed by the physical limitations on the quantity of documents and other materials that an individual could carry or otherwise have within reach at the time of arrest. See *Chimel* v. *California*, 395 U.S. 752, 763 (1969) (police may search incident to arrest only the space within an arrestee's "'immediate control,'" which means "the area from within which he might gain possession of a weapon or destructible evidence").

Although the exception is justified by the need to "'seize weapons' and 'to prevent the destruction of evidence'" (*Chimel*, 395 U.S. at 764), the Court has not required a showing that those justifications were in fact present in order to uphold a search incident to arrest. "The authority to search the person incident to a lawful custodial arrest * * * does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect." *United States* v. *Robinson*, 414 U.S. 218,

235 (1973). The Court has said that the arrest "for at least a reasonable time and to a reasonable extent" takes the arrestee's "own privacy out of the realm of protection from police interest in weapons, means of escape, and evidence." *United States* v. *Edwards*, 415 U.S. 800, 808-809 (1974) (internal quotation marks omitted).

But the "reasonableness" of that across-the-board rule—in terms of the types and quantity of information that may be accessed by the government—plainly rested in large measure on the practical limitations on the reach of such a search. Those practical limitations are not present in the case of smartphones.

That significant change in the amount and types of information routinely within an individual's possession is highly relevant to the application of the Fourth Amendment in this context. Cf. *Jones*, 132 S. Ct. at 964 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment) (finding a Fourth Amendment violation because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period"); *id.* at 956 (Sotomayor, J., concurring) (recognizing that the "attributes of GPS monitoring" must be taken into account "when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements"); *Quon*, 130 S. Ct. at 2629 ("[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior"

producing expectations of privacy protected by the Fourth Amendment).

Here, as in *Jones*, the consequences of new technology render unreasonable the application of a legal standard formulated in a dramatically different factual context. The search-incident-to-arrest exception may allow the seizure of a smartphone, but it cannot justify automatic review by the government—without a warrant and showing of probable cause—of the myriad types of information contained in the device.

C. This Court Should Consider The Search-Incident-To-Arrest Issue In The Context Of A Search Implicating The New Capabilities Of Today's Smartphones.

As petitioner explains (Pet. 11-13), the lower courts have reached conflicting conclusions regarding the application of the search-incident-to-arrest exception in the context of searches of cell phone contents. This Court's intervention is needed to resolve that conflict.

The Court's analysis of the constitutional issue will be aided substantially by granting review in a case—such as this one—that involves a smartphone and a search of photographs and other information that today's technology allows to be stored on a cell phone. See Pet. 2-3. That factual setting will enable the Court to assess the effect of this new technology, and particularly how the technology alters the "pre-computer age, * * * practical" protections of privacy. *Jones*, 132 S. Ct. at 963 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment).

A number of lower court decisions have involved old-style cell phones with limited capabilities in which the government search involved review of what probably were the only categories of information contained on the phone: the call log—the list of the telephone numbers called from the cell phone and numbers from which calls were received by the cell phone—and, in some cases, the list of names and phone numbers inserted by the phone's owner. *E.g.*, *Commonwealth* v. *Phifer*, 979 N.E.2d 210, 216 (Mass. 2012).

Some judges upholding searches of the contents of old-style cell phones have analogized the search to review of an address book contained in the arrestee's pocket. *E.g.*, *Wurie*, 2013 WL 2129119, at *15 (Howard, J., dissenting). Whatever the merits of that analogy, it obviously does not apply to the millions of pages of information that can be stored on a smartphone but could not be carried by any individual in physical form.

The case in which the Solicitor General seeks review of a search-incident-to arrest decision, *United States* v. *Wurie*, No. 13-212 (filed Aug. 15, 2013), suffers from this defect. It involves an old-style phone and a search limited to the call log and name/phone number listings.

Indeed, the government observed in its court of appeals rehearing petition in *Wurie* that the phone involved was "a simple 'flip' phone rather than a computer-like 'smartphone,'" and that "[t]o the extent that some cell phones may implicate more serious privacy concerns * * * those concerns are not present in this case, which involved a brief examination of the call log of a flip phone." Government's Pe-

tition for Rehearing En Banc at 2, 6, *United States* v. *Wurie*, No. 11-1792 (1st Cir. July 16, 2013).

In this Court, however, the government seeks a broad rule applying the search-incident-to-arrest exception to *all* information stored on *all* types of cell phones. See, *e.g.*, No. 13-212 Pet. 11, 16 (advocating a "bright-line rule" authorizing the search of cell phones notwithstanding the "large amount of personal information" stored on smartphones). But the government's observations in its rehearing petition regarding the narrow factual context presented in *Wurie* explain why that case is an inappropriate vehicle for addressing that broad question.

As one commentator observed in comparing the present case with *Wurie*,

> [g]iven that the argument for treating cell phones differently from physical items hinges on the storage capacity and services available through smartphones, I think it would be very helpful for the Court to take a case involving a smartphone instead of a more primitive model. * * * * Reviewing a case with an earlier model phone would lead to a decision with facts that are atypical now and are getting more outdated every passing month.

Orin Kerr, *Two Petitions on Searching Cell Phones Reach the Supreme Court*, The Volokh Conspiracy, Aug. 19, 2013, available at http://www.volokh.com/2013/08/19/doj-files-cert-petition-in-wurie/.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

ANDREW J. PINCUS
Counsel of Record
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com
Counsel for Amici Curiae

AUGUST 2013

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

No. 13-132

In The
Supreme Court of the United States

DAVID LEON RILEY,
Petitioner,

v.

STATE OF CALIFORNIA,
Respondent.

On Petition for a Writ of Certiorari to the California Court of Appeal, Fourth District

BRIEF OF CONSTITUTIONAL ACCOUNTABILITY CENTER AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

DOUGLAS T. KENDALL
ELIZABETH B. WYDRA*
**Counsel of Record*
BRIANNE J. GOROD
CONSTITUTIONAL
ACCOUNTABILITY CENTER
1200 18th St., NW, Suite 501
Washington, D.C. 20036
(202) 296-6889
elizabeth@theusconstitution.org
Counsel for Amicus Curiae

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTEREST OF *AMICUS CURIAE* 1

SUMMARY OF ARGUMENT 1

ARGUMENT 5

THE COURT SHOULD GRANT REVIEW BECAUSE THE CELL PHONE SEARCH PERMITTED BY THE COURT BELOW IS INCONSISTENT WITH THE TEXT AND HISTORY OF THE FOURTH AMENDMENT 5

A. The Framers Viewed the Fourth Amendment as a Fundamental Protection Against the Use of "General Warrants" 6

B. Permitting Broad Searches of Cell Phones Incident to Arrest Undermines the Fundamental Protections of the Fourth Amendment 15

CONCLUSION 20

TABLE OF AUTHORITES

Page(s)

Cases

Arizona v. Gant,
556 U.S. 332 (2009) 17

Berger v. State of New York,
388 US 41 (1967) 11

Boyd v. United States,
116 U.S. 616 (1886) 11

Chandler v. Miller,
520 U.S. 305 (1997) 16

Chimel v. California,
395 U.S. 752 (1969) 17

City of Ontario, Cal. v. Quon,
130 S. Ct. 2619 (2010) 19

Marcus v. Search Warrants of Property at 104 East Tenth Street, Kansas City, Mo.,
367 U.S. 717 (1961) 8

Maryland v. King,
133 S. Ct. 1958 (2013) 7, 12, 13, 16, 17

United States v. Chadwick,
431 U.S. 1 (1977) 6

United States v. Wurie,
--- F.3d ---, 2013 WL 2129119
(1st Cir. May 17, 2013) 19

TABLE OF AUTHORITIES—continued

Page(s)

Warden, Md. Penitentiary v. Hayden,
387 U.S. 294 (1967) 16

Wilkes v. Wood,
98 Eng. Rep. 489 (1763) 10

Constitutional Provisions and Legislative Materials

U.S. CONST. amend. IV 6, 19

Annals of Congress, 1st Cong. 1st Sess. (1789)..... 14

Books, Articles, and Miscellaneous

Akhil Reed Amar, *The Bill of Rights as a Constitution*, 100 YALE L.J. 1131 (1991)..... 10

WILLIAM CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING (2009) ... *passim*

Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999) ... 11, 13

Charles E. MacLean, *But, Your Honor, A Cell Phone Is not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37 (2012) 18

Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925 (1997)..... 9

TABLE OF AUTHORITIES—continued

Page(s)

Letter from James Madison to George Eve (Jan. 2, 1789), *at* http://bit.ly/134r6nw 14

Hon. M. Blane Michael, Madison Lecture, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. REV. 905 (2010) ..... *passim*

JAMES OTIS, IN OPPOSITION TO WRITS OF ASSISTANCE (1761) 9

Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165 (2008) 18

JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES (1833) .. 6, 7

INTEREST OF AMICUS CURIAE[1]

Amicus Constitutional Accountability Center (CAC) is a think tank, public interest law firm, and action center dedicated to fulfilling the progressive promise of our Constitution's text and history. CAC works in our courts, through our government, and with legal scholars to improve understanding of the Constitution and preserve the rights and freedoms it guarantees. CAC has a strong interest in ensuring that the Constitution applies as robustly as its text and history require and accordingly has an interest in this case.

SUMMARY OF ARGUMENT

The Petition for a Writ of Certiorari in this case presents the important question whether the Fourth Amendment permits police officers to conduct a warrantless search of the digital contents of a person's cell phone seized from that person at the time of arrest. As the Petition demonstrates, this is a question of fundamental importance on which the federal courts of appeals and state appellate courts are plainly divided, and it therefore merits this Court's review. This brief in

---

[1] Counsel for all parties received notice at least 10 days prior to the due date of *amicus*'s intention to file this brief; all parties have consented to the filing of this brief. Under Rule 37.6 of the Rules of this Court, *amicus* states that no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amicus* or its counsel made a monetary contribution to its preparation or submission.

support of the Petition emphasizes the importance of the constitutional question presented by demonstrating that the warrantless search of a cell phone such as the one in this case, even incident to a lawful arrest, conflicts with the text and history of the Fourth Amendment.

When the Framers drafted the Fourth Amendment, which broadly provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," and that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," they were responding, in large part, to the British use of "general warrants" and "writs of assistance." These warrants and writs lacked any specificity about the people or items to be searched and were not predicated on any individualized suspicion; essentially unlimited in scope, these warrants and writs allowed the officers executing them virtually unfettered discretion to engage in broad searches of a person's home and the personal papers and effects in that home.

As early as the 1600s, the use of such warrants came under attack in Great Britain. They were decried as the "worst instrument of arbitrary power," and popular opposition to their use quickly solidified as they were used to harass critics of the Crown and trample personal liberty. The British nonetheless continued to use general warrants, including in the colonies. During the

1700s, colonial opposition to the use of such warrants grew, and their use was one of the grievances that prompted the call for independence from British rule.

Concerns about the abusive use of general warrants continued in the post-colonial period, and calls for the Nation's new Constitution to include an explicit prohibition on the use of general warrants produced what would become the Fourth Amendment. The text of the Fourth Amendment, both as originally drafted and in the form that was ultimately adopted, reflects the Framers' staunch opposition to the use of general warrants. It required not only that all searches be reasonable, but also that all warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." This uniquely detailed text enshrines a specific prohibition against general warrants in our Nation's charter, and reflects the Framers' more general concern that government officers not be able to search a person's home, papers, and effects in the absence of some individualized, justified suspicion that a specific search would produce evidence of wrongdoing. Stated simply, the Framers wanted to strip the government of the arbitrary power to rifle through a person's belongings in the hope of finding something incriminating.

The practice permitted by the court below violates this fundamental Fourth Amendment precept. The contents of Petitioner David Riley's cell phone were searched without a warrant and without exigent circumstances, first at the scene of

his arrest and then hours later at the police station. As the Petition demonstrates, none of the traditional justifications for warrantless searches incident to a lawful arrest can justify the search of the digital contents of Riley's cell phone—the phone had been removed from Riley upon his arrest, thus eliminating any concern about destruction of evidence, and it is difficult to see how the text messages, emails, photos, and other digital contents of the phone could have posed any threat, let alone an imminent threat, to the arresting officers' safety. To the contrary, as the detective who searched Riley's phone hours after the arrest acknowledged, he dug through "'a lot of stuff" on the phone specifically "'looking for evidence.'" Pet. 3 (citing Tr. 176, 193). This is precisely the type of search for which the Constitution demands a warrant.

By permitting law enforcement officers to look through the contents of an arrestee's cell phone without a warrant and in the absence of recognized exigent circumstances, the decision below invites law enforcement to engage in the same sort of generalized searches that the Framers abhorred—and adopted the Fourth Amendment to prevent. Because modern cell phones generally contain vast stores of information, including private communications and photographs, the intrusion into an individual's privacy when police rummage through the contents of a smart phone is substantial. Indeed, because a person may store much of his most private information on his cell phone, the invasion of privacy involved in such searches will often be similar in degree to (if not

more substantial than) the intrusion on privacy that occurred when individuals' homes—and their personal papers and effects—were searched by overreaching British colonial officers during the Founding era.

Amicus urges the Court to grant *certiorari* and reverse the erosion of the Fourth Amendment's fundamental protections countenanced by the decision below.

ARGUMENT

THE COURT SHOULD GRANT REVIEW BECAUSE THE CELL PHONE SEARCH PERMITTED BY THE COURT BELOW IS INCONSISTENT WITH THE TEXT AND HISTORY OF THE FOURTH AMENDMENT

Amicus urges this Court to grant *certiorari* to clarify the scope of the Fourth Amendment's protections when law enforcement officers search a person's cell phone incident to a lawful arrest. By permitting the police to search the digital contents of an arrestee's cell phone without first obtaining a warrant, even after the phone has been removed from the arrestee, the California Supreme Court and other courts around the country have given the police unfettered discretion to engage in broad invasions of individual privacy. It was just this sort of generalized search, undertaken without probable cause or particularized suspicion, that the Fourth Amendment was adopted to prevent. This Court should grant *certiorari* and clarify that the Fourth Amendment's text and history prohibit the

warrantless searches permitted by the court below.

A. The Framers Viewed the Fourth Amendment as a Fundamental Protection Against the Use of "General Warrants"

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the text suggests, the Framers incorporated this fundamental safeguard of liberty into the Constitution to limit the discretion of government officers to engage in general searches unsupported by specific, articulable suspicion, and to prevent the broad invasions of privacy that such searches could entail. This safeguard was "indispensable to the full enjoyment of the rights of personal security, personal liberty, and private property." Joseph Story, Commentaries § 1895.

The Fourth Amendment's broad protections were in large part a response to specific abuses the Framing generation had suffered under British rule—namely, the use of "general warrants" and "writs of assistance" that lacked specificity as to the person and place to be searched and were not based on any individualized suspicion. *See, e.g.*, *United States v. Chadwick*, 433 U.S. 1, 7-8 (1977) ("It cannot be doubted that the Fourth Amendment's

commands grew in large measure out of the colonists' experience with the writs of assistance and their memories of the general warrants formerly in use in England."); *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting) (noting that the Framers "despised" the use of general warrants); Hon. M. Blane Michael, Madison Lecture, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 905, 906 (2010) (noting that "the British Crown's unbridled power of search . . . is at the center of the rich history that led to the adoption of the Fourth Amendment"); *id.* at 907 ("The Fourth Amendment owes its existence to furious opposition in the American colonies to British search and seizure practices, particularly in the area of customs enforcement."). As Joseph Story observed, the Fourth Amendment's "introduction into the amendments was doubtless occasioned by the strong sensibility excited, both in England and America, upon the subject of general warrants almost upon the eve of the American Revolution." Story, *supra*, § 1895. Such warrants were despised by Americans as the tools of an arbitrary and unlimited government, used to harass and oppress the people.

General warrants had long been used in Great Britain. For example, the Act of Frauds of 1662 "empowered customs officers in England to enter 'any house, shop, cellar, warehouse or room, or other place' and to 'break open doors, chests, trunks and other package[s]' for the purpose of

seizing any 'prohibited and uncustomed' goods." Michael, *supra*, at 907.[2] These warrants were also used to limit the publication of materials critical of the government. *See Marcus v. Search Warrants of Property at 104 East Tenth Street, Kansas City, Mo.*, 367 U.S. 717, 726 (1961) (noting that in the mid-seventeenth century, the Parliament's asserted need for "a broad search and seizure power to control printing" resulted in the issuance of warrants that "often gave the most general discretionary authority"); *see also id.* at 724 ("Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power.").

As early as the mid-1600s, the use of these general warrants came under attack in Great Britain when Edward Coke "became the first of many English legal thinkers to deny the legality of general warrants." William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning 105 (2009). "By the end of the century, at least four legal treaties had mentioned Coke's language against general warrants as legal fact," *id.* at 121, and the popularity of Coke's views continued to spread in the ensuing years, as other "legal treaties recited Coke on general warrants as doctrine," *id.*

Despite the growing opposition to the use of general warrants in Great Britain, they remained

---

[2] In 1696, "the broad enforcement powers in the 1662 Act" were extended "to customs officers in the colonies, authorizing the officers to conduct warrantless searches at their discretion." Michael, *supra*, at 907.

the standard method of search in the colonies as of the mid-eighteenth century, *see* Tracy Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. Rev. 925, 940 (1997). Colonial opposition to the use of general warrants was galvanized by a series of events on both sides of the Atlantic on the eve of the American Revolution.

In the high-profile Paxton's Case, for example, a group of Boston merchants challenged customs officials' use of general warrants, Cuddihy, *supra*, at 380, attacking them as "'the worst instrument of arbitrary power, the most destructive of English liberty . . . that ever was found in an English law-book.'" Michael, *supra*, at 908. The merchants' attorney, James Otis, argued that such warrants "place[] the liberty of every man in the hands of every petty officer." James Otis, *In Opposition to Writs of Assistance*, http://bartleby.com/268/8/9 (last visited July 24, 2013); *see* Michael, *supra*, at 908 (noting that Otis called the writ of assistance an "'instrument[] of slavery on the one hand, and villainy on the other'"). According to Otis, writs of assistance could be legal only if they were much more specific, providing for the "search [of] *certain houses* &c. *especially set[ting] forth*, . . . *upon oath made* . . . by the person who asks *that he suspect such goods to be concealed in* THOSE VERY PLACES HE DESIRES TO SEARCH." Cuddihy, *supra*, at 377-78 (quoting Brief of Otis, *Paxton's Case* (Mass. Sup. Ct. 24-26 Feb. 1761), *Massachusetts Spy*, Thu., 29 Apr. 1773 (vol. 3, no. 117), p. 3, col. 1). Although the writs in *Paxton's Case* were granted, the decision prompted public resistance, and the

Massachusetts legislature responded by reducing the judges' salaries and passing a law requiring the use of specific warrants. Cuddihy, *supra*, at 403-04; *cf.* Michael, *supra*, at 908 (noting that this case "galvanized support for what became the Fourth Amendment").

In the years that followed, colonial opposition to general warrants continued to grow, in part in response to events in Great Britain. When a publication was released that criticized the King, the British Secretary of State issued a general warrant to authorize sweeping searches of forty-nine individuals who might be responsible. John Wilkes, the primary target of the investigation, sued those responsible for executing the warrant. In one of the resulting trials, Chief Justice Pratt of the Court of Common Pleas declared general warrants to be "illegal, and contrary to the fundamental principles of the constitution." *Wilkes v. Wood*, 98 Eng. Rep. 489, 499 (1763). This case was widely covered in American newspapers, and "the reaction of the colonial press to that controversy was intense, prolonged, and overwhelmingly sympathetic to Wilkes." Cuddihy, *supra*, at 538; *see id.* at 539 (discussing the scope of the coverage in the colonial press); *id.* at 538 (noting that a "revulsion to general warrants ensued in the colonies" following the Wilkes controversy); *cf.* Akhil Reed Amar, *The Bill of Rights as a Constitution*, 100 Yale L.J. 1131, 1176 (1991) ("Madison's choice of language [in the Fourth Amendment] may well have been influenced by the celebrated 1763 English case of Wilkes v. Wood, one of the two or three most important

search and seizure cases on the books in 1789." (internal footnote omitted)).

Despite the growing opposition to general warrants, Parliament in 1767 again authorized their use in the colonies. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 566 (1999). Some of the local courts in the colonies resisted, refusing to issue the broad, general writs authorized by the Act and instead issuing the more specific warrants lauded by Otis. Cuddihy, *supra*, at 519. But "[g]eneral warrants and affiliated methods were still central to colonial search and seizure in 1776." *Id.* at 538.

The colonists' animosity toward general warrants was one of the grievances that caused them to seek independence from Great Britain. As John Adams would later remark, Otis's fiery attack on the practice in *Paxton's Case* "was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." Michael, *supra*, at 909 (quoting Letter from John Adams to William Tudor (March 29, 1817) *in* The Works of John Adams 247-48 (Boston, Little Brown & Co. 1856)). Indeed, the colonists attached great importance to the issue of general warrants as they contemplated breaking ties with Great Britain. *See, e.g.*, *id.* at 911 ("the First Continental Congress in 1774 included customs searches under general writs of assistance in its list of grievances against Parliament"); *see also Berger v. State of N.Y.*, 388 U.S. 41, 58 (1967) (noting that the use of general warrants "was a motivating factor behind the Declaration of

Independence"); *Boyd v. United States*, 116 U.S. 616, 625 (1886) (describing the debate in which Otis's speech occurred as "perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country").

After the War for Independence was won, the colonists' fight to end the use of general warrants continued. Although their use initially remained common in the new Nation, Cuddihy, *supra*, at 603 ("General warrants proliferated and remained the keystone of American laws and practices regarding search and seizure until at least 1782."), the "specific warrant ultimately won out," *id.* By 1784, Vermont and half the thirteen states had "formulated constitutions with restrictions on search and seizure," although the precise formulations of those restrictions varied. *Id.*; *see King*, 133 S. Ct. at 1980-81 (Scalia, J., dissenting) (quoting, for example, the Virginia Declaration of Rights § 10, which provided that "general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed," or to search a person "whose offence is not particularly described and supported by evidence," "are grievous and oppressive, and ought not be granted").[3]

---

[3] The introduction of constitutional prohibitions on the use of general warrants did not result in the complete elimination of such searches in the States, Cuddihy, *supra*, at 624, 628, but these constitutional provisions were nonetheless the "direct ancestors" of the Fourth Amendment, *id.* at 603.

When the Framers gathered to draft the new federal Constitution, concerns about potential abuses of governmental authority through the use of general warrants were raised. *See* Davies, *supra*, at 583. Indeed, the Constitution's failure to provide any protection against general warrants was a favorite topic of Anti-Federalist writers, at least 15 of whom penned objections to the Constitution on that ground. Cuddihy, *supra*, at 674; *see id.* ("The general warrant attracted the earliest and heaviest criticism."); *King*, 133 S. Ct. at 1981 (Scalia, J., dissenting) ("Antifederalists sarcastically predicted that the general, suspicionless warrant would be among the Constitution's 'blessings'"). Patrick Henry, for example, "warned that the new Federal Constitution would expose the citizenry to searches and seizures 'in the most arbitrary manner, without any evidence or reason.'" *King*, 133 S. Ct. at 1981 (Scalia, J., dissenting) (quoting 3 Debates on the Federal Constitution 588 (J. Elliot 2d ed. 1854)). Another critic of the new Constitution described "the absence of security against [general] warrants as part of an 'extraordinary' failure by Congress to safeguard the people's rights." Cuddihy, *supra*, at 674. James Otis's sister, Mercy Otis Warren, joined the fight, "assail[ing] writs of assistance" as "'a detestable instrument of arbitrary power.'" *Id.* at 677.

Several state ratifying conventions requested more explicit protection. The Fourteenth Amendment of Virginia's proposed Bill of Rights reflected Anti-Federalists' concerns about general warrants, providing, in pertinent part, that "all

general warrants to search suspected places, or to apprehend any suspected person, without specially naming or describing the place or person, are dangerous and ought not to be granted." *Id.* at 684. New York, North Carolina, and Rhode Island copied Virginia's search and seizure amendment with minimal alteration. *Id.* at 685. The arguments presented in favor of including an express prohibition on general warrants in the federal constitution received consistent and nationwide newspaper coverage, and "[t]he magnitude of that publicity indicated the emergence of a consensus for a comprehensive right against unreasonable search and seizure." *Id.* at 686.

Although the Federalists initially believed that there was no need to add a Bill of Rights to the Constitution, by 1789, James Madison had decided the Constitution should be amended to expressly protect a number of "essential rights" not expressly protected in the new Constitution, including the "security against general warrants." Letter from James Madison to George Eve (Jan. 2, 1789), *at* http://bit.ly/134r6nw. The initial text of his proposed amendment made clear the importance that he attached to individualized and particularized suspicion as predicates for governmental searches: "The rights of the people to be secured in their persons, their houses, their papers, and their other property from all unreasonable searches and seizures, shall not be voided by warrants . . . not particularly descrybing the places to be searched, or the persons or things to be seized." 1 *Annals of Cong.* 452 (1789) (Joseph

Gales ed., 1790). The language was subsequently modified in committee, but the requirement of specific warrants remained materially unchanged. Cuddihy, *supra*, at 695-97.

The Fourth Amendment thus enshrines in our national charter the Framers' opposition to generalized searches that were not predicated on any individualized suspicion. The practice condoned by the court below violates that core Fourth Amendment principle, as the next section demonstrates.

B. Permitting Broad Searches of Cell Phones Incident to Arrest Undermines the Fundamental Protections of the Fourth Amendment

As just noted, the Fourth Amendment was a response, in significant part, to the abusive use of general warrants by the British, but its adoption also reflected a broader concern about the intrusions into privacy that could result if the government enjoyed unlimited discretion to search people's homes and belongings. Michael, *supra*, at 906 (noting the "broader purpose of the Amendment: to circumscribe government discretion"); Cuddihy, *supra*, at 679 (noting an Anti-Federalist "desire to divest the central government not only of [the general warrant] but of all relatives of it that jeopardized privacy"). Thus, as this Court has repeatedly recognized, a core concern of the Fourth Amendment is ensuring that the government has individualized suspicion about

wrongdoing before it intrudes on a person's privacy. *See, e.g.*, *Chandler v. Miller*, 520 U.S. 305, 308 (1997) (The Fourth Amendment's "restraint on government conduct generally bars officials from undertaking a search or seizure absent individualized suspicion."); *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (The Fourth Amendment was "a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies, and was intended to protect against invasions of 'the sanctity of a man's home and the privacies of life' from searches under indiscriminate, general authority." (internal citation omitted)); *King*, 133 S. Ct. at 1982 (Scalia, J., dissenting) ("suspicionless searches are *never* allowed if their principal end is ordinary crime-solving").

The practice permitted by the court below violates this fundamental Fourth Amendment precept. By allowing the police to search the contents of an individual's cell phone without a warrant, it permits exactly the sort of generalized search lacking in particularized suspicion (and the concomitant invasion of privacy) that the Fourth Amendment's requirement for particularized warrants was supposed to prevent. That such searches are triggered by an arrest does little to limit the government's discretion because, as the Petition notes, "arrests are often triggered by legal infractions as minor as failure to abide by the vehicle code." Pet. 14.

Moreover, that the individual whose phone is being searched was arrested is not sufficient to

justify the broad invasion of privacy that the court below condoned. As this Court recently noted, the fact that a person is in custody following arrest cannot justify all searches, regardless of the level of privacy invaded, *King*, 133 S. Ct. at 1979, and as the Petition demonstrates, the traditional justifications for searches incident to arrest have no bearing once the cell phone has been removed from the arrestee's control, *see* Pet. 22-24 (explaining that a phone's digital contents "can never threaten officer safety," and "once officers separate an arrestee from his phone, they can eliminate any risk that he might destroy digital evidence on the phone"); *see also Chimel v. California*, 395 U.S. 752, 763 (1969) (setting out the twin purposes of searches incident to arrest, *viz.*, "remov[ing] any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape" and "seiz[ing] any evidence on the arrestee's person in order to prevent its concealment or destruction"); *Arizona v. Gant*, 556 U.S. 332, 339 (2009) ("If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply."). Moreover, because of the vast stores of information that are generally saved on modern cell phones, the invasion of privacy inherent in such a search is significantly greater than the invasion involved in previous search-incident-to-arrest cases, involving, for example, physical containers with much more limited and physical contents. *See* Pet. 9, 25-28.

Modern cell phones are unique, after all, in

that they permit individuals to carry significant amounts of personal information and documents that would previously have been kept in the home and office. Indeed, they are like computers in their ability to store vast amounts of information, *see, e.g.*, Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 Ga. L. Rev. 1165, 1172 (2008) (noting that cell phones have been described as "microcomputers"); *id.* at 1201 ("The more advanced devices are practically hand-held computers with telephone capabilities, giving the user access to a wealth of public and private data stored online and in the device's memory."),[4] and thus will often contain not only phone call records and a rolodex of the owner's contacts (both professional and personal), but also thousands of email messages and texts, photographs, even personal notes. *See, e.g.*, Pet. 10. The smartphone that was searched in this case was "capable of accessing the internet, capturing photos and videos, and storing both voice and text messages, among other functions," *id.* at 2, and the police search exposed private text messages, the phone's contacts list, photographs, and videos, *id.* at 3.

In other words, many documents and effects

---

[4] The storage capacities of modern cell phones are staggering. For example, "modern cell phones are capable of storing at least sixty-four gigabytes of private information equaling four million pages of Microsoft Word documents." Charles E. MacLean, *But, Your Honor, A Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L. Rev. 37, 42 (2012).

that would once have been stored physically in a person's home are often now stored in digital form, and a search of a person's cell phone thus invites an invasion of personal privacy that is little different than the invasion of privacy produced by searches of people's homes and papers at the Founding. *See United States v. Wurie*, --- F.3d ---, 2013 WL 2129119, at *7 (1st Cir. May 17, 2013) ("Just as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government's proposed rule would give law enforcement automatic access to 'a virtual warehouse' of an individual's 'most intimate communications and photographs without probable cause' if the individual is subject to a custodial arrest, even for something as minor as a traffic violation."); *cf. City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

The Framers adopted the Fourth Amendment to ensure that the people would be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. This Court should grant *certiorari* to clarify the scope of the Fourth Amendment's protections and hold that its text and history do not permit police officers to conduct a warrantless search of the digital contents of an individual's cell phone seized from the person

at the time of arrest.

CONCLUSION

For the foregoing reasons, *amicus* urges the Court to grant the Petition for a Writ of Certiorari.

Respectfully submitted,

DOUGLAS T. KENDALL
ELIZABETH B. WYDRA*
*Counsel of Record
BRIANNE J. GOROD
CONSTITUTIONAL
ACCOUNTABILITY CENTER
1200 18th Street NW, Suite 501
Washington, D.C. 20036
(202) 296-6889
elizabeth@theusconstitution.org
Counsel for Amicus Curiae

August 2013

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Petition for a Writ of Certiorari
to the California Court of Appeal, Fourth District

BRIEF OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

JEFFREY T. GREEN
CO-CHAIR, AMICUS COMMITTEE
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1501 K Street, NW
Washington, D.C. 20005
(202) 736-8291

BRONSON D. JAMES*
BRONSON JAMES LLC
Box 205
14925 S.W. Barrows Rd., Ste 109
Beaverton, OR 97007
(503) 515-6216
bj@bronsonjames.com

Counsel for Amicus Curiae

*Counsel of Record

August 30, 2013

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF AMICUS CURIAE 1

REASONS FOR GRANTING THE WRIT 2

I. The Modern Smartphone Is A Historically Unique Device With Profound Societal Implications. 2

A. Distributed Computing And Cloud Data Give Mobile Computing Infinite Capacity 6

B. Smartphone Usage Is Now Societally Ubiquitous 7

II. This Case Presents The Best Vehicle For This Court's Analysis. 11

III. The Smartphone In This Case, Unlike The Phone In *Wurie*, May Possess First Amendment Overtones Affecting The Fourth Amendment Analysis 12

IV. Lower Court Divisions Make This The Right Time For This Court To Consider The Issue 14

V. The Nature And Societal Use Of Mobile Data Compels The Result That The Fourth Amendment Prohibits The Warrantless Search Of The Data Of A Cell Phone Incident To Arrest 15

CONCLUSION 19

TABLE OF AUTHORITIES

Page(s)

CASES

Arizona v. Gant, 556 U.S. 332 (2009) 18

Bell v. Wolfish, 441 U.S. 520 (1979) 17

Bertot v. Sch. Dist. No. 1, Albany Cnty., Wyo., 613 F.2d 245 (10th Cir. 1979) 14

Channel 10, Inc. v. Gunnarson, 337 F. Supp. 634 (D.Minn. 1972) 14

Fed. Election Comm'n v. Wis. Right to Life, Inc., 551 U.S. 449 (2007) 14

Jones v. United States, 357 U.S. 493 (1958) 17

Katz v. United States, 389 U.S. 347 (1967) 16

Oliver v. United States, 466 U.S. 170 (1984) 16

Roaden v. Kentucky, 413 U.S. 496 (1973) 13, 14

Robinson v. Fetterman, 378 F. Supp. 2d 534 (E.D. Pa. 2005) 13

Rossignol v. Voorhaar, 316 F.3d 516 (4th Cir. 2003) 13

State v. Nordlund, 53 P.3d 520 (Wash. Ct. App. 2002). 13

States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) 12

United States v. Chadwick, 433 U.S. 1 (1977) 15

United States v. Edwards, 415 U.S. 800 (1974) 16

United States v. Rabinowitz, 339 U.S. 56 (1950) 18

United States v. Robinson, 414 U.S. 218 (1973) 16

United States v. Wurie, No. 11-1792, 2013 WL 2129119 (1st Cir. May 17, 2013), *petition for cert. filed* Aug. 15, 2013 (No. 13-212) 11, 16

OTHER AUTHORITIES

Aaron Smith, *Smartphone Ownership – 2013 Update*, Pew Research Ctr.'s Internet & Am. Life Project (June 5, 2013) 8

Amanda Lenhart, *Cellphones and American Adults* (2010) 10

David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205 (2009) 7

Gary Krakow, *Smartphones, Meet the Terabyte*, The Street (Feb. 17, 2009) 5

Harris Interactive, *Mobile Mindset Survey* (2012) 11

Int'l Telecomm. Union, *Measuring the Information Society* (2010) 8

M. Wesley Clark, *Searching Cell Phones Incident to Arrest*, FBI L. Enforcement Bull., Feb. 2009 15

Mary Kimani, *A Bank in Every African Pocket*, United Nations African Renewal (Jan. 2008). 10

SETEC Investigations, *How Many Pages per Gigabyte and Megabyte?* (2006) 3

INTEREST OF AMICUS CURIAE[1]

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of the United States advancing the mission of the nation's criminal defense lawyers to ensure justice and due process for persons accused of crime or other misconduct. NACDL was founded in 1958.

NACDL has a nationwide membership of approximately 10,000 and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, active U.S. military defense counsel, law professors and judges. NACDL provides amicus assistance on the federal and state level in cases that present issues of importance, such as the one presented here, to criminal defendants, criminal defense lawyers, and the proper and fair administration of criminal justice.

---

[1] Counsel of Record for the parties received timely notice of amicus curiae's intent to file this Brief. Petitioner filed blanket consent to the filing of amicus curiae briefs on August 15, 2013. A letter of consent from the Respondent to the filing of this brief has been lodged with the Clerk of the Court pursuant to Rule 37.2. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

REASONS FOR GRANTING THE WRIT

This Court should grant review because the smartphone has assumed a unique role in modern society. The mobile computing revolution has fundamentally altered how people incorporate technology and data into their everyday lives. This case, unlike other petitions before this court, most completely presents the question of how a smartphone is to be treated under the Fourth Amendment.

I. The Modern Smartphone Is A Historically Unique Device With Profound Societal Implications.

Any smartphone is capable of storing digital information locally, meaning that the physical device is the repository of the information. It is when we are discussing localized storage that analogizing these devices to containers is arguably appropriate. However, the volume of information stored strains that analogy.

The base unit of measurement of all stored digital data is the bit, which is a binary value of 0 or 1. The byte, which is the smallest unit of data storage, is eight bits. Eight bits yields 2^8, or 256 permutations of 0 or 1 – that number is the amount necessary to store a single alphanumeric such as the letter "A."

In the early days of digital storage, space was measured in kilobytes (KB), or 1000 bytes. The standard 5.25" floppy disk in production in 1982 held

1185.5KB. That capacity was quickly replaced with the megabyte (MB), or 1,000,000 bytes. The 3.5" floppy disk in widespread use by 1987 held 1.44MB, or 1,440,000 bytes.

The number of bytes required to produce a digital document varies depending upon the program that created and stores the document. In addition to the text content, various packet and formatting bytes are lost to the program. A rough average of physical pages per megabyte, however, is provided in Table 1 (below).

Table 1: Average Pages of Data per MB[2]

Document Type	Pages per MB
MS Word files	63
Email files	97
Microsoft Excel files	161
Lotus 1-2-3 files	280
PowerPoint files	17
Text Files	662
Image Files	15

[2] These estimates are industry standard and widely reproduced. SETEC Investigations, *How Many Pages per Gigabyte and Megabyte?* (2006), http://www.setecinvestigations.com/resources/techhints/Pages_per_Gigabyte.pdf.

By the mid-1990's, the 3.5" floppy disk gave way to the CDROM as the industry standard for portable data. The standard 74-minute CDROM contained 333,000 sectors, each housing 2,048 bytes, for a total storage capacity of 650MB. One CDROM replaced over 450 3.5" floppy disks.

By the millennium, the DVD had supplanted the CDROM as the default removable storage mechanism. DVD storage varied upon the model of DVD drive reader; the most basic, DVD-1, contained 1.46 Gigabytes (GB), a Gigabyte equaling one billion bytes. The highest standard, DVD-18, contained 17.08 GB of data.

In the 1990's, along with CDs and DVDs, digital storage devices began to include cell phones, Personal Digital Assistants, and thumb drives. Those devices, too, grew in storage capacity at an astonishing rate. In 2007, when Apple launched the iPhone, the initial model held 4 GB of data. Three years later, Apple released the iPhone 4.0 which held 32 GB of data. The current model holds 64 GB.

That number continues to grow. In 2009, data storage manufacturers announced the development of the next-generation data storage architecture for phones, SDXc (Secure Digital Extended Capacity). The iPad2, one of the first devices to employ SDXc, is available in a 128 GB configuration. And SDXc is expected to push iPhones and other smartphones into the area currently reserved for laptop computers: the terabyte. Smartphones with storage in the 1-2 TB

range are expected within this decade. [3] To place that number in perspective, a 1 TB phone could contain all the data listed in Table 2 (below), *all at once*, and still only be three-quarters full:[4]

Table 2: Localized Data Capacity of 1 TB Devices

120 hours of DVD quality video (approx. 100 GB)
720 hours of audio recordings (approx. 100 GB)
22,200 high-res color photographs (approx. 100 GB)
6,300,000 pages of MS Word documents (approx. 100 GB)
160,000,000 pages of Excel spreadsheets (approx. 100 GB)
97 million emails (approx. 100 GB)

With SDXc as the new storage architecture standard, individuals will truly have the capacity to store an entire lifetime's data in their pocket. Videos

---

[3] *See* Gary Krakow, *Smartphones, Meet the Terabyte*, The Street (Feb. 17, 2009), http://www.thestreet.com/story/10464195/smartphones-meet-the-terabyte.html; and *Terabyte Capacity for Smartphones* at http://www.telecomasia.net/content/terabyte-capacity-smartphones-0.

[4] Determining digital storage capacity is simply a mathematical calculation. To aid in that calculation, petitioner refers this court to a number of data storage computational aids online. *See e.g,* http://www.unitarium.com/data or http://www.lexbe.com/hp/Pages-Megabyte-Gigabyte.aspx.

of one's wedding, the birth of one's children, and every family reunion and school performance will easily fit on the device. Assuming 10 one-minute voicemails a day, everyday each year, the phone will hold over eleven years of voicemail messages. If you took three photographs of your child everyday of his life, from birth through high-school graduation, they would all fit on the phone with room to spare. It would easily contain not just every document you authored, but every page of every document you have ever read. Finally, it would hold every email and text message you have ever received or sent – *for your entire lifetime.*

A. Distributed Computing And Cloud Data Give Mobile Computing Infinite Capacity

Even though the capacity of localized storage strains traditional human conceptualizations of size, it is dwarfed by a cellphone's secondary storage mechanism: cloud data.

Cloud data is not stored locally, at least not all of it. Rather, the physical device contains tags, or permanent conduits (i.e., saved encrypted passwords and account numbers) to data stored outside the physical device, on distributed systems shared across the internet. As one commentator summarized:

> "Experts have coined the term 'Web 2.0' to describe the shift in Internet usage from consumption to participation and metaphorically refer to this virtual platform as 'the cloud,' where users interact with Internet

> applications and store data on distant servers rather than on their own hard drives."

David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing,* 93 Minn. L. Rev. 2205, 2205 (2009).

Freed from physical restrictions, cloud computing allows cellphones to achieve infinite data capacity. By distributing data storage outside the device, and using the local storage to house conduits and tags to that data, pulling it down to the device on demand, there is literally nothing that cannot be stored on a device that fits in one's pocket. And most new cellphone applications are utilizing this technology.

For the iPhone, for example, Bank of America, U.S. Bank, and all major financial institutions have applications which link the phone via cloud computing to the user's bank account, including full histories of deposits, payments, loans, credit, etc. GEICO, Allstate, and all major insurers have similar apps linking the phone to insurance account information. And applications such as HealthCloud and GoogleHealth are designed to link the mobile device directly with offsite health records maintained by doctors and hospitals.

B. Smartphone Usage Is Now Societally Ubiquitous

The development of mobile data has represented one of the largest technological revolutions in human history. In 2002, roughly 16%

of the world's population owned a cellphone. In just seven years, that number quadrupled:

> "By the end of 2009, there were an estimated 4.6 billion mobile cellular subscriptions, corresponding to 67 per 100 inhabitants globally (Chart 1). Last year, mobile cellular penetration in developing countries passed the 50 per cent mark reaching an estimated 57 per 100 inhabitants at the end of 2009. Even though this remains well below the average in developed countries, where penetration exceeds 100 per cent, the rate of progress remains remarkable. Indeed, mobile cellular penetration in developing countries has more than doubled since 2005, when it stood at only 23 per cent."

International Telecommunications Union, *Measuring the Information Society* ix (2010).[5] The vast majority of Americans now own a cell phone – approximately 91% as of June 2013. Of those cell phone owners, 61% own smartphones.[6]

For many, mobile data is replacing traditional methods of conducting one's life. Mobile banking, for example, is increasingly replacing brick-and-mortar bank branches. This is particularly true in developing countries. India, parts of central Asia,

---

[5] Report available at: http://www.itu.int/ITU-D/ict/publications/idi/material/2010/MIS_2010_without_annex_4-e.pdf.

[6] *See* Aaron Smith, *Smartphone Ownership – 2013 Update*, Pew Research Ctr.'s Internet & Am. Life Project, 2 (June 5, 2013), *available at* http://www.pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx.

and large sections of Africa have bypassed the traditional infrastructure development of the West, and leapt straight into a cellular based model.

> "Across Africa, only 20 per cent of families have formal bank accounts, according to a World Bank survey. In Tanzania the percentage is as low as 5 per cent, and in Liberia 15 per cent.
>
> "But the proliferation of mobile telephone services around the continent has opened a new way to extend financial services * * * In the few countries where they have emerged, companies such as M-Pesa can use any phone or phone card to provide affordable services to customers wherever there is a mobile phone signal.
>
> " * * * * *
>
> "According to Mohsen Khalil, the World Bank's director of global ICT, Wizzit's operation is one of the most innovative approaches to mobile banking, since it specifically targets the poor. If this model works in South Africa, he says, the World Bank will help the company expand coverage within and beyond the country. 'We may be looking here at . . . the most effective way to provide social and economic services to the poor.'"

Mary Kimani, *A Bank in Every African Pocket*, United Nations African Renewal, 1-2 (Jan. 2008).[7]

Additionally, for a growing segment of America, accessing information via a portable device has become the norm:

> "No longer just for communicating and planning while away from home or the workplace, the cell phone is increasingly a landline substitute. Recent research by the Pew Research Center suggests that 23% of Americans have only a cell phone available for making calls and another 17% have a landline but receive most of their calls on their mobile phone. For some subgroups, the findings are even more dramatic; nearly one-third (30%) of Hispanics and 49% of adults 25-29 are cell-only."

Amanda Lenhart, *Cellphones and American Adults* 2 (2010).[8]

So integral has the cellphone become to day-to-day living that the same study found that 65% of all cellphone owners actually sleep with their phone. *Id.* at 11. A 2012 survey found that 58% of phone owners check their phones at least once an hour, in bed

---

[7]Study available at: http://www.un.org/africarenewal/magazine/january-2008/bank-every-african-pocket.

[8] Report available at http://pewinternet.org/~/media//Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf.

before sleep and immediately upon waking. Harris Interactive, *Mobile Mindset Survey*, 2012.[9]

II. This Case Presents The Best Vehicle For This Court's Analysis.

In addition to this case, this court has before it a petition for certiorari in *United States v. Wurie*, No. 11-1792, 2013 WL 2129119 (1st Cir. May 17, 2013), *petition for cert. filed* Aug. 15, 2013 (No. 13-212). However this case is the better vehicle for this court to analyze the issues.

As discussed above, storage capacity, Internet connectivity, and its use as a point of connectivity in all aspects of life make the smartphone the defining device of the mobile computing age. This case involves precisely that device. Here the defendant had a Samsung smartphone, containing data in a variety of formats, including photographs and video.

Wurie, however, involves an older generation "flip phone." Those devices are anachronisms, the principal use being voice communication, not data transmission. The *Wurie* phone is not the hub of connectivity represented by the smartphone in this case. It could not be used to access health records, financial data, or an Internet search. And at least one lower court has suggested that the nature of the data may affect the Fourth Amendment analysis.

---

[9] Report available at https://www.lookout.com/resources/reports/mobile-mindset.

States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012)

In terms of a technological spectrum, the phone in Wurie is closer to a 1980's pager than a modern smartphone. In short, the technology at issue in *Wurie* has already expired beyond its shelf life. Although mobile computing will certainly continue to evolve, it will never return to an age where Internet connectivity and social networking is lacking. *Wurie* asks this court to evaluate the Fourth Amendment in the context of a technology that is fixed in a point in the past that will never return.

III. The Smartphone In This Case, Unlike The Phone In *Wurie*, May Possess First Amendment Overtones Affecting The Fourth Amendment Analysis.

Lower courts have noted that, by their range of capabilities, ease of access, and societal saturation, smartphones are the quintessential free speech instruments of our age:

> "The trial court aptly described a personal computer as 'the modern day repository of a man's records, reflections, and conversations.' CP at 200. Thus, the search of that computer has first amendment implications that may collide with fourth amendment concerns. When this occurs, we closely scrutinize compliance with the particularity and probable cause requirements. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 98 S.Ct. 1970, 56 L.Ed.2d 525

> (1978); *Stanford v. Texas*, 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965); *Perrone*, 119 Wash.2d at 547, 834 P.2d 611 ('Where a search warrant authorizing a search for materials protected by the First Amendment is concerned, the degree of particularity demanded is greater[.]'). *See also Stenson*, 132 Wash.2d at 692, 940 P.2d 1239 (search warrants for documents are generally given closer scrutiny because of potential for intrusion into personal privacy)."

State v. Nordlund, 53 P.3d 520, 525 (Wash. Ct. App. 2002).

This Court has afforded heightened protection to First Amendment instruments. The warrantless seizure of such material is a form of prior restraint, a long disfavored practice. *Roaden v. Kentucky*, 413 U.S. 496, 503 (1973) (when an officer "br[ings] to an abrupt halt an orderly and presumptively legitimate distribution or exhibition" of material protected by the First Amendment, such action is "plainly a form of prior restraint and is, in those circumstances, unreasonable under Fourth Amendment standards."). *See also Rossignol v. Voorhaar*, 316 F.3d 516, 522 (4th Cir. 2003) (Where sheriff's deputies suppressed newspapers critical of the sheriff "before the critical commentary ever reached the eyes of readers, their conduct met the classic definition of a prior restraint.").

In an age when anyone with a cellphone can blog, post to newsgroups, capture still photo and video, send correspondence, and use all form of social mass communication, an officer's warrantless seizure of an individual's first amendment instrumentality must be accorded a stricter standard. *See Robinson v.*

Fetterman, 378 F. Supp. 2d 534, 541 (E.D. Pa. 2005) (By restraining an individual from "publicizing or publishing what he has filmed," officer's "conduct clearly amounts to an unlawful prior restraint upon [] protected speech."); *see Channel 10, Inc. v. Gunnarson*, 337 F. Supp. 634, 637 (D.Minn. 1972) ("it is clear to this court that the seizure and holding of the camera and undeveloped film was an unlawful 'prior restraint' whether or not the film was ever reviewed."). The warrantless seizure of material protected by the First Amendment "calls for a higher hurdle in the evaluation of reasonableness" under the Fourth Amendment. *Roaden*, 413 U.S. at 504.

This Court has noted that, when faced with a close call, "the First Amendment requires [courts] to err on the side of protecting * * * speech rather than suppressing it." *Fed. Election Comm'n v. Wis. Right to Life, Inc.*, 551 U.S. 449, 457 (2007). *See also Bertot v. Sch. Dist. No. 1, Albany Cnty., Wyo.*, 613 F.2d 245, 252 (10th Cir. 1979) ("We prefer that governmental officials acting in sensitive First Amendment areas err, when they do err, on the side of protecting those interests.").

IV. Lower Court Divisions Make This The Right Time For This Court To Consider The Issue.

State and Federal courts are deeply divided over whether the Fourth Amendment permits the police to search the digital contents of an arrestee's cell phone incident to arrest. The petition before this Court thoroughly details that divide.

This issue will not go away, or work itself out. The smartphone has become the central locus of interaction with one's entire digital life. And simultaneously it has become an irresistible target for law enforcement. "It is the rare arrestee today who is not found in possession of a cell phone."[10]

Both law enforcement and citizens need clarity from this court in determining what extent cell phones are protected by the Fourth Amendment.

V. The Nature And Societal Use Of Mobile Data Compels The Result That The Fourth Amendment Prohibits The Warrantless Search Of The Data Of A Cell Phone Incident To Arrest.

Petitioner thoroughly sets out this Court's incident to arrest jurisprudence. That jurisprudence was created in a time when tangible objects were the dominant source of evidence against a defendant. But the mobile computing revolution has altered that fundamental assumption.

A smartphone, and it's near infinite data capacity, is not the equivalent of a footlocker as in *United States v. Chadwick*, 433 U.S. 1 (1977). Likewise, simply because technology has allowed us to contain a wealth of data in our pocket, does not

---

[10] M. Wesley Clark, *Searching Cell Phones Incident to Arrest*, FBI L. Enforcement Bull., Feb. 2009, at 25, *available at* http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2009-pdfs/february09leb.pdf.

mean that the privacy protections of smartphones are the equivalent of clothing as under *United States v. Robinson*, 414 U.S. 218 (1973) or *United States v. Edwards*, 415 U.S. 800 (1974).

Amicus agrees with Petitioner that the framework of *Chadwick*, *Edwards*, and *Robinson* cannot adequately govern mobile data. As the First Circuit noted, this Court, "more than thirty-five years ago, could not have envisioned a world in which the vast majority of arrestees would be carrying on their person an item containing not physical evidence but a vast store of intangible data – data that is not immediately destructible and poses no threat to the arresting officers." *Wurie*, 2013 WL 2129119, at *10.

A smartphone, with all the data it can access, and all the privacy expectations accompanying that data, is not the constitutional equivalent of a crumpled cigarette pack. Ultimately the categories that have built up around the Fourth Amendment cannot blindly control. As this Court has said:

> "But this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places."

Katz v. United States, 389 U.S. 347, 351 (1967). The touchstone of the analysis is always the reasonable expectation of privacy. *Oliver v. United States*, 466 U.S. 170, 171 (1984).

The exceptions to the warrant requirement are just that – exceptions. They represent the outlier, not the norm. Those exceptions "have been jealously and carefully drawn, and search incident to a valid arrest

is among them." *Jones v. United States*, 357 U.S. 493, 499 (1958).

The applicability of an exception does not rest upon rigid categories, but upon its reasonableness, and its fundamental purpose.

> "The test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted."

Bell v. Wolfish, 441 U.S. 520, 559 (1979).

The fundamental purpose behind the search incident to arrest exception, as Justice Frankfurter stated, is necessity:

> " * * * In plain English, the right to search incident to arrest is merely one of those very narrow exceptions to the 'guaranties and immunities which we had inherited from our English ancestors, and which had from time immemorial been subject to certain well-recognized exceptions arising from the necessities of the case.' * * *
>
> " * * * Its basic roots, however, lie in necessity. What is the necessity? Why is search of the arrested person permitted? For two reasons: first, in order to protect the arresting officer and to deprive the prisoner of potential means of escape, * * * and, secondly, to avoid

> destruction of evidence by the arrested person."

United States v. Rabinowitz, 339 U.S. 56, 71 (1950) (Frankfurter, J. dissenting).

When that necessity is not present, a search under the exception is no longer reasonable. As this Court held in *Gant*:

> "If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply."

Arizona v. Gant, 556 U.S. 332, 339 (2009).

In the case of smartphones, the claim of necessity is illusory. Because mobile computing devices can hold a lifetime of data, and provide a wealth of information about activities and locations, they will always, in theory, be potential repositories of evidence for any conceivable crime.

Faced with the smartphone, the exception threatens to eclipse the Fourth Amendment itself. The warrant exception becomes a proxy for an exploratory search of an entire lifetime's worth of private information on the hope that some parcel will incriminate a defendant. This cannot be the rule. The Fourth Amendment demands more protection for the societal privacy accorded these devices and their contents.

This Court should grant review in this case and set forth, for the benefit of law enforcement and the citizenry, how the search incident to arrest exception functions in a world now dominated by

smartphones, as opposed to cigarette packs and footlockers.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

JEFFREY T. GREEN
CO-CHAIR, AMICUS COMMITTEE
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1501 K Street, NW
Washington, D.C. 20005
(202) 736-8291

BRONSON D. JAMES*
BRONSON JAMES LLC
Box 205
14925 S.W. Barrows Rd., Ste 109
Beaverton, OR 97007
(503) 515-6216
bj@bronsonjames.com

Counsel for Amicus Curiae

*Counsel of Record

August 30, 2013

JOINT APPENDIX

Supreme Court, U.S.
FILED
MAR 3 - 2014
OFFICE OF THE CLERK

No. 13-132

IN THE
Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On a Writ of Certiorari
to the California Court of Appeal,
Fourth District

JOINT APPENDIX

Christine Levingston Bergman*
Deputy Attorney General
OFFICE OF THE CALIFORNIA
ATTORNEY GENERAL
110 West A Street, Suite 1100
San Diego, CA 92186-5266
(619) 645-2247
Christine.Bergman@doj.ca.gov

Attorney for Respondent

Jeffrey L. Fisher *
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@law.stanford.edu

Attorney for Petitioner

* *Counsel of Record*

March 2014

Petition for Certiorari filed July 30, 2013
Certiorari granted January 17, 2014

TABLE OF CONTENTS

Relevant Docket Entries 1

Transcript of Proceedings (October 25, 26, 28, 29, 2010 and November 1, 2, 2010) 3

Testimony of Charles Dunnigan 4

Testimony of Duane Michael Malinowski 10

Analysis by the Court 21

Transcript of Proceedings (February 28 and March 1, 2011) 25

Transcript of Proceedings (March 2, 2011) 27

Testimony of Duane Michael Malinowski 28

Transcript of Proceedings (March 3, 2011) 34

Testimony of Scott Barnes 35

People's Exhibit Number 39 42

People's Exhibit Number 40 43

People's Exhibit Number 41 44

RELEVANT DOCKET ENTRIES

Date Filed	Docket Text
06/14/2010	Superior Court of the State of California for the County of San Diego. Information filed.
09/27/2010	Superior Court of the State of California for the County of San Diego. Defendant's motion to suppress filed.
10/08/2010	Superior Court of the State of California for the County of San Diego. First Amended Information filed.
10/25/2010	Superior Court of the State of California for the County of San Diego. Suppression hearing commenced.
10/26/2010	Superior Court of the State of California for the County of San Diego. Suppression hearing concluded; motion to suppress denied.
10/29/2010	Superior Court of the State of California for the County of San Diego. Trial commenced.
11/18/2010	Superior Court of the State of California for the County of San Diego. Trial concluded; Court announced the hung jury.
12/09/2010	Superior Court of the State of California for the County of San Diego. Second Amended Information filed.

02/28/2011	Superior Court of the State of California for the County of San Diego. Renewed Motion to Suppress denied.
02/28/2011	Superior Court of the State of California for the County of San Diego. Second Trial commenced.
03/10/2011	Superior Court of the State of California for the County of San Diego. Second Trial concluded; jury finds defendant guilty as charged.
05/20/2011	Court of Appeal of California, Fourth Appellate District. Notice of appeal filed.
01/16/2013	Court of Appeal of California, Fourth Appellate District. Oral Argument heard.
02/08/2013	Court of Appeal of California, Fourth Appellate District. Decision issued.
03/18/2013	Supreme Court of California. Petition for review filed.
05/01/2013	Supreme Court of California. Petition for review denied.

IN THE SUPERIOR COURT OF
THE STATE OF CALIFORNIA IN AND FOR
THE COUNTY OF SAN DIEGO

Department 38 & 59
Before Hon. Laura W. Halgren, Judge

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. DAVID RILEY & DONTE HADDOCK, Defendants.	CT SCD 226240 DA ACR883

REPORTER'S TRANSCRIPT
October 25, 26, 28, 29, November 1 & 2, 2010

APPEARANCES

For the People — BONNIE DUMANIS,
District Attorney
BY: JAMES SIMMONS, JR., DDA
330 W. Broadway
San Diego, CA

For Defendant Riley — OFFICE OF ASSIGNED COUNSEL
BY: EDWARD W. KINSEY, Esq.
7760-H Fay Ave, Ste 303
La Jolla, CA 92037

For Defendant Haddock — OFFICE OF ASSIGNED COUNSEL
BY: GARY ROBERTS, Esq.
PO Box 620321
San Diego, CA 92162

MICHAEL SHANE GALLIVAN
Official Reporter, CSR5169
San Diego, California

* * * *

[DIRECT EXAMINATION OF CHARLES DUNNIGAN]

[BY MR. SIMMONS]:

[111:7]

Q. So you contact Mr. Riley after pulling the vehicle over, correct?

A. Yes, sir.

Q. Can you tell us what happened?

A. I ran a driver's license check from his California Driver's License. And I discovered that his driver's license was suspended.

Q. What did you do at that time?

A. I returned to the vehicle. I asked him to step out of the car. Prior to doing so, I noticed that he reached for his right leg – his right pocket. And I told him not to do that. He simply told me he was reaching for his cell phone. He had made a previous statement that he had been arrested prior for a weapons charge. Based on that statement and his movement toward his left, or right leg, I asked him to step out of the car so I could conduct a pat-down search. And the other purpose was to remove him from the vehicle because once I noticed his license was suspended my plan was to tow the vehicle. So I removed him from the vehicle to search the car prior to impound.

Q. At what point during this contact did Mr. Riley made [sic] make the statement to you about being arrested in the past for [112] weapons charges.

A. Prior to me having him exit the vehicle. I typically ask everybody I stop if they are on probation, parole or if they have been arrested before. It was subsequent to some question like that probably.

Q. You said your intent was to impound the vehicle?

A. Yes, sir.

Q. And why was that?

A. Anytime I stop somebody with a suspended license, with a few exceptions, the car gets towed.

Q. And that's what you, and that's what you were planning in this case?

A. Yes, sir.

Q. Did you have another officer come and cover you or assist you in this?

A. Yes, I did. Officer Matt Ruggiero.

Q. And he was not there during the initial stop, is that correct?

A. That's correct.

Q. At what point did Officer Ruggiero –

A. Ruggiero.

Q. – Ruggiero, at what point did he arrive?

A. I couldn't tell you exactly when, but sometime between probably when I was talking to Mr. Riley on the curb, after I had him exit the vehicle.

Q. Now, as part of the impound of a vehicle, do you normally conduct an inventory impound search of that vehicle?

[113]

A. Yes, sir.

Q. What's the purpose of that?

A. Well, a couple of things. One is to limit liability for the City, so that someone doesn't later claim there were items in the vehicle that aren't there when they go get their car back, that's number one. And that's primarily why we search the vehicle and make sure that the condition it's impounded in is the condition it's returned to the owner.

Q. And you didn't search that vehicle yourself that day, correct?

A. No, sir.

Q. And were you aware of Mr. Riley's involvement with any shootings at the time that you pulled him over?

A. Not at that time, no.

Q. Were you aware of any possible gang connections with Mr. Riley at the time you pulled him over?

A. Not at that time, no.

Q. Later on, after Mr. Riley was arrested, did you contact Det. Malinowski?

A. Yes, I did.

Q. What was the reason for that?

A. Once I, once we found the guns and realized that Mr. Riley had some gang connections, based on some paraphernalia we found on his person and the car, and that was basically tokens that are carried by gang members to show their gang affiliation –

MR. KINSEY: Objection. Lack of foundation. Move to strike. [114]

THE COURT: Sustained as to the last part, as to what a token is.

BY MR. SIMMONS:

Q. What was the reason for calling Det. Malinowski?

A. Well, we found the guns. We realized that Mr. Riley was associated with a street gang. And Det. Malinowski is a detective that works that area for street gangs.

Q. So you weren't – let me rephrase this. You didn't contact Det. Malinowski before you pulled the vehicle over, is that correct?

A. No, sir.

Q. Now, you mentioned that you saw some items that you considered to be gang paraphernalia?

A. Yes, sir.

Q. Can you tell us what items you are talking about?

A. Found a green bandana. Green is specifically, I'll say, used by the Lincoln Park street gang to identify with a color associated with a gang. And then a pair of Converse, little miniature key chain Converse, which is also a known item carried by gang members to show their affiliation with their gang.

Q. And what color were the Converse, if you know?

A. I think there was one red one and one green one.

Q. And during your arrest of Mr. Riley did you have occasion to look at his cell phone?

A. Yes, I did.

Q. And what, if anything, did you see inside?

A. I noticed that everything that started with a K was [115] preceded by a C. And it's my experience that gang members typically write a C and a K to stand for Crip Killer. Sometimes they will have it on their hat or tattoos on their person, somewhere to signify their gang affiliation as a Blood set. They put the C in front of the K, which on the street means Crip Killer.

Q. And just so we're clear, where was the bandana found at on Mr. Riley?

A. Well, it was, I believe, in his right pocket. I don't remember if it was the right, or the front or the back. It's in my report.

Q. I'll ask you a few more questions. Did you take any statements from Mr. Riley that day?

A. No, sir.

Q. So he never made any admissions or anything to you?

A. No, sir.

Q. And Officer Ruggiero conducted the search that we talked about?

A. Yes, sir.

Q. Did Officer Ruggiero share with you the results of his search?

A. Yes, he did.

Q. What did you see?

A. He showed me where a white sock concealing a handgun was clearly obvious. A handgun was stuffed inside an athletic sock. Because of the shape of the sock, it was wrapped around the sides of a gun, I clearly recognized it to be the shape of [116] gun, as well as I could see through a hole in the sock the color black. At that point, after he pointed it out to me, he actually secured Mr. Riley first. He pointed it out to me. He removed the item, removed a gun from inside the athletic sock. There was another gun in a [sic] another sock, a blue sock below that in the engine compartment.

MR. SIMMONS: I have no further questions at this time.

THE COURT: Cross-examine?

MR. KINSEY: Thank you, your Honor. [116:9]

* * * * *

[175:18]

DIRECT EXAMINATION [OF DUANE MICHAEL MALINOWSKI]

BY MR. SIMMONS:

Q. Good afternoon, Det. Malinowski. You are a sworn San Diego police officer?

A. Correct.

Q. Were you on duty on August 22nd of last year?

A. Yes.

Q. And did you get called out to the fight – actually, on that date did you come into contact with a defendant or individual by the name of David Riley?

A. Yes. That was on my day off. I was on call. And I [176] was called in I was notified of his arrest and called in to conduct an interview and process the arrest.

Q. You were actually called into the police station?

A. Yes, I was on my day off.

Q. Did you come into contact with Mr. Riley that day?

A. Yes.

Q. And did you talk to him?

A. Yes.

Q. And just so we're clear, you weren't involved in the stop or arrest of Mr. Riley, is that correct?

A. I was not.

Q. So you, you are called in. You come in contact with Mr. Riley. Did you have an opportunity to look through his cell phone?

A. Yes.

Q. And how did that come about?

A. The officers provided me with his cell phone when I asked for the property that they found on him. And I went through his cell phone.

Q. And what, if anything, did you find?

A. There's a lot of stuff on his cell phone, but one of the things that caught my eye was some short video clips of some kids or young men, looked like they were boxing, like, street boxing.

Q. And what do you mean by "street boxing"? I just [177] want it for clarification purposes.

A. What guys do in the street to show their toughness or whatever, whatever reason they do it. They might have a problem between each other, or just to show how tough they are. Part of the initiation to gang, whatever, there will be a couple guys go out, bare fists. Sometimes they wear riders, which are like batting gloves or car-repair type gloves, the leather ones. They go at it. There are rules. If somebody goes down, you don't jump on top and start beating them. It's a boxing match without the gloves, basically.

Q. Looking at the video, did you see anyone – or did you see Mr. Riley in that video at all?

A. You could not see Mr. Riley in the video. You could hear Mr. Riley and could you [sic] see his – on one of the videos you could see his car parked there, because the boxing was near his car.

Q. And what could you hear him saying in the video?

A. He said a lot of things, "Get brackin', Blood," things.

MR. KINSEY: Objection. Lack of foundation with regard to what Mr. Riley said.

THE COURT: As to whether it was him, you mean?

MR. KINSEY: Yes.

THE COURT: Sustained.

BY MR. SIMMONS:

Q. All right. Before that day had you been in contact with Mr. Riley before?

A. Yes.

[178]

Q. How many times, approximately?

A. At least twice.

Q. During both of those opportunities, and well, all three, including the 22nd of August, did you have a chance to speak with Mr. Riley?

A. Yes.

Q. Did you have a chance to hear him speak?

A. Oh, yes.

Q. And based on hearing him speak, when you looked through those videos were you able to recognize his voice?

A. Yes.

Q. And I'm just going to ask this question: How were you able to recognize it was his voice?

A. Just like I can recognize other people's voices that I've spoken to.

Q. And based on your experience with Mr. Riley, talking with him and hearing what you thought to be his voice on the video, what did you hear him say?

A. He was saying things, "Get him blood. Brack and Blood on Lincoln," things like that, "Come on Lincoln," encouraging the boxing match.

Q. Now, did it appear to you that the individuals in the boxing match were from the same gang, for lack of a better term?

A. Based on what was said – but based on the actions, I mean, they respected the street boxing rules of, you know, somebody gets hit – actually in one of the fights somebody loses a necklace, one of the swings, like, tears off a [179] necklace. And they kind of stop and let the person collect the necklace.

Q. Is that typical between rivals, to allow something like that to happen?

A. Oh, no. It's something like that, when it goes there, they will fight until they knock them to the ground. They are not going to care about a necklace.

Q. As far as the individuals involved in the fighting did you recognize any of those individuals?

A. At that day that I viewed the video, I did not.

Q. Did you recognize anyone at a later date?

A. Yes.

Q. Who did you recognize?

A. Mr. Haynes and Mr. Haddock.

Q. So you saw both of them in that video?

A. Correct.

Q. What were they doing?

A. They were involved in the boxing. They were the boxing participants.

Q. And that cell phone was impounded into evidence?

A. Yes, it was.

Q. Were you able to download the video to a separate source at all?

A. Yeah. The videos were downloaded, along with a bunch of photos. And I know Det. Hunter did that. A lot of that through RCFL, which is our computer technician people, for other pending cases of Mr. Riley's.

Q. Do you know if that was ever submitted in this case?

[180]

MR. KINSEY: Objection. Move to strike with other cases.

THE COURT: Based on foundation?

MR. KINSEY: Relevance.

THE COURT: Overruled for the motion.

BY MR. SIMMONS:

Q. Let me ask you another question. Other – excuse me for a second.

I have nothing further at this time.

THE COURT: All right. Mr. Kinsey, you may cross-examine.

MR. KINSEY: Thank you.

CROSS EXAMINATION

BY MR. KINSEY:

Q. Det. Malinowski, what time were you called in to process the arrest?

A. It was early in the morning. I think it was already, I believe he was already downtown. And they called me from downtown.

Q. Do you recall about what time of day it was?

A. It was in the morning, before noon.

Q. Before noon?

A. Correct.

Q. And what did you do when you were called in to process the arrest, what exactly did you do?

A. I saw Mr. Riley in the sallyport. He was in a car. I spoke to the officers, were briefed from the officers on the arrest. Set up the interview room. And then I believe I actually escorted Mr. Riley upstairs to the interview room. [181] Got all his personal information. Read him his rights. Didn't want to talk to me. Escorted him back downstairs. And released

him back to the officers. And then went through his personal property and stuff.

Q. I'm sorry?

A. And then went through his personal property.

Q. And you had recognized him from twice previously?

A. Yeah. Mr. Riley, I've seen pictures of him, numerous pictures of him on the internet, Myspace photos, things like that. And Mr. Riley has – you are probably not going to like it – but an infamous reputation in the Lincoln Park street gang.

Q. So, but you actually had contact with him, personal contact with him twice?

A. Twice prior to that day that I can recall, yes.

Q. And what was the context of those contacts?

A. The other one was an arrest where he was arrested with a gun up off El Cajon Boulevard some months earlier. I think it was a revolver. The officers brought him down and called me and I interviewed him on that case. And then another time was at 5100 Logan. He was contacted by some officers when a – I believe it was James Callaway ran from his convertible Mustang and Mr. Riley stayed behind. I think he was on probation for possession of a firearm at the time, or he had just discharged that probation case.

Q. During any of those contacts did Mr. Riley ever admit to being a gang member?

A. No, I can't recall. I would have to look at all the [182] contacts. I talked to a lot of people.

Q. He never told you, "I claim Lincoln Park," or anything like that, did he?

A. Again, I would have to look through all the contacts.

Q. When you viewed the videos on the cell phone and saw the street boxing, was anybody bleeding?

A. I don't recall any bleeding, because most of the time they kind of backed away. They didn't want to get hit. I don't recall any real good strikes. They were kind of swinging not to – not like you would swing in a ring like if you really wanted to knock somebody out.

Q. They weren't really boxing, they were kind of messing around?

A. No, they were trying to connect. You could see they were definitely trying to connect. I don't think – just looking at the video, didn't seem like either one of them really had a heart to take a punch.

Q. And you, on August 22nd had suspected that Mr. Riley was involved in a shooting from August 2nd, correct?

A. Correct.

Q. And you suspected Mr. Riley to be part of that shooting as of August 2nd, correct?

A. Correct.

Q. Did you, as part of your capacity as a gang detective, disseminate information to other officers in the department that you suspected Mr. Riley to be involved in that shooting?

[183]

A. Yes.

Q. How did you do so?

A. I talked to the GST officers at lineup.

Q. GST being?

A. Gang Suppression Team officers.

Q. Gang Suppression Team?

A. Correct.

Q. Was that information communicated to patrol officers in the area?

A. I have no idea what they did with that information.

Q. Were you looking for Mr. Riley on August 22nd?

A. I was looking to talk to him from August 2nd through the 22nd, but was I actively looking for him? No. Was I kicking in doors and doing probation searches, things of that nature? No.

Q. You wanted to find him since August 2nd?

A. Correct.

Q. Did you – when you disseminated the information to the gang suppression team, which officers did you disseminate that information to?

A. Whoever was in the lineup room.

Q. How many officers would that be?

A. It varies day to day. I – you know, sometimes there's eight working, sometimes there's 21 working.

Q. And you don't recall – strike that. How often did you disseminate this information to the GST, was it every day?

A. No, it was within a few days after the shooting had [184] occurred.

Q. Every day for a few days after?

A. The days that I was able to attend the lineup and –

Q. Doing something else?

A. Yes.

Q. Is it common practice for the members of the gang suppression team to disseminate want information to patrol officers?

A. Usually if there's printed fliers. If I go in, like, wanted, like I have probable cause to arrest somebody for the case, not just question them about it, if I know there's a warrant in the system or probation violation where maybe the warrant is not in the system, I will prepare a flier and I will hand that and say, "Hey give that to the senior officers. Give it to the mid-city officers," things like that. In this case I didn't do that.

Q. You did not facilitate the dissemination of the information to anyone beyond members of the Gang Suppression Team?

A. Correct, because he was not arrestable.

Q. But you suspected him to be involved in a shooting?

A. Yeah. I expect [sic] a lot of people for doing a lot of things, it doesn't mean I can go arrest him.

Q. You were looking for the guns involved in that shooting?

A. Correct.

MR. KINSEY: Thank you. I have nothing further.

[184:28]

* * * * *

[193:18]

CROSS EXAMINATION [OF DUANE MICHAEL MALINOWSKI]

BY MR. KINSEY:

Q. Det. Malinowski, did you have a warrant to search that cell phone?

A. No. I went through, I went through it looking for evidence, because I know gang members will often video themselves with guns or take pictures of themselves with the guns. I have knowledge, I've seen pictures where guys are arrested with the gun, pictures with them with the firearms on the phone. I was looking for further evidence to prove that he was in possession of those firearms that the officers found [194] inside the car or videos of what they found inside the vehicle.

Q. Mr. Riley was under arrest and going to jail at that point?

A. Correct.

Q. And you had possession of the phone?

A. Correct.

Q. And you suspected that that phone probably contained some evidence of gang involvement?

A. I had no idea. It would just be like I was searching through his pockets, looking for a green bandana.

Q. That phone wasn't going anywhere?

A. No, I still had it in my possession at the time yes.

Q. And it's been in police possession ever since, right?

A. I don't know. Det. Hunter has been dealing with it with his case, so it's probably still there.

MR. KINSEY: Thank you. No further questions.

[194:20]

* * * * *

[453:10]

THE COURT: I did look – I read *Gant* earlier, so actually what I wanted to do was go on. If we are not dealing with anything else, I will go ahead and rule on the cell phone now. I'm prepared to do that.

I will just note that I have reviewed multiple authorities, including a Law Review article or a portion of it. But in particular I did read the cases cited by Mr. Kinsey, including *United States versus Park*, which is a Northern District California case, and *U.S. versus Wall*, which is the Southern District of Florida. I also looked at *U.S. versus Ortiz*, which is the Seventh Circuit. That's an old one from 1996, but finding that the transient and disappearing nature of information received by a pager constitutes exigency, which is slightly different than a cell phone.

U.S. versus Finley is probably the most current circuit court case, that's Fifth Circuit, 2007. And that case found that search of a cell phone was valid because search incident to arrest allows search of containers found on the person.

Then, by contrast, there's a case out of the Supreme Court in Ohio, *State versus Smith*, where they found it [454] impermissible because they found it wasn't a closed container and there's a privacy interest that goes beyond an address book or a pager.

So those cases sort of set up the conflicting views. What I went back to finally is looking at *People versus Diaz*, which of course is not something that is authoritative in the state because it's a court of appeal opinion which the Supreme Court granted review. The Supreme Court granted review and held in part to wait for the ruling in *Gant*. But after looking at *Gant*, I don't think that the analysis there changes the analysis in *Diaz*. And *Diaz* does lay out the, the two issues that we're looking at.

I think under *Chimel*, C-h-i-m-e-l, an arresting officer can search a person arrested to remove weapons that later might be used in order to resist arrest or effect escape. And the police can then arrest – search the arrestee's person and the area within his immediate control to remove weapons and secure evidence. So originally that was the, the purpose of *Chimel*, to essentially remove weapons and insure safety of bystanders and prevent destruction of evidence. Over the years it's [sic] has expanded.

Where I think we are at on this analysis is whether this falls within the *Edwards* line of cases that would say that a cell phone is something that is part of the person or does this fall within *Chadwick*, is it a container that is perhaps near the person, but not part of the person, so to speak? And the analysis that was done in the *Diaz* case I think overall makes sense.

[455]

As I think we've mentioned in having discussion on this, courts do allow and have allowed items on the person to be searched, including wallets, address books, papers and the like. Cell phones do contain personal information, but really no more so than wallets and purses and address books. It's just that they hold a lot more than those things do. The cell phone in this case was on Mr. Riley's person. There was testimony that he went to reach for it. It was in his pants leg pocket or on the right side. And because it was on his person at the time of arrest, under case authority it can be concluded that was taken out of the realm from protection for police interest for a reasonable time following the arrest. That comes from *United States versus Passaro*, P-a-s-s-a-r-o, at 624 Fed 2d, at Page 944, and looking at also *United States versus Edwards*, at 415 U.S., at Pages 808, 809.

The – what gives the officer the right to do the search is the lawful arrest. And Mr. Riley was lawfully arrested. And in the case of a lawful arrest, a full search of the person is an exception to the warrant requirement of the fourth amendment and is reasonable under that amendment. And citing for that *United States versus Robinson*, 414 U.S., at Page 235.

So in this case it is clear that looking at the cell phone is for investigative purposes, it has nothing to do with weapons. But it was an investigation relating to the crime for which he was arrested, which was the finding of the guns in the car. And Malinowski testified that in his experience persons and gang members do take photos of themselves and [456] their crimes and he expected there could be such photos on the cell phone. So I think that it was an investigation related to the arrest. And because the cell phone was

on the person, it's allowed under the authorities I've cited.

So I will allow the People to use – I'm not – let's put it this way: This is in connection with the motion to suppress, so I'm denying the motion to suppress the cell phone or evidence found on it. * * * * [456:8]

* * * * *

IN THE SUPERIOR COURT OF
THE STATE OF CALIFORNIA IN AND FOR
THE COUNTY OF SAN DIEGO

Department 38 Honorable Laura W. Halgren, Judge

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. DAVID RILEY, Defendant.	CASE NO. SCD226240 TRIAL (PAGES 501 through 658)

REPORTER'S TRANSCRIPT
February 28 and March 1, 2011

APPEARANCES:

For the People:

BONNIE DUMANIS
District Attorney
By: JAMES SIMMONS
Deputy District Attorney
330 West Broadway
San Diego, California
92101

For the Defendant: EDWARD W. KINSEY
Attorney at Law
7760-H Fay Avenue,
Suite 303
La Jolla, California 92037

Reported By: DENISE CARRILLO, RPR,
CRR, CSR No. 9626
San Diego, California

* * * *

[517:26]

[THE COURT]:

And there also was a motion relating to the cell phone evidence. And based on the recent California Supreme Court Case – the name escapes me at the moment. [518] It was pending when we argued it last, but the ruling by the Supreme Court was consistent with what this court held. So the cell phone evidence remains admissible.

MR. KINSEY: I would like to renew my motion, but I am familiar with the court's citation to that case, though I don't know the name of it either.

THE COURT: The defense objections are noted and overruled for the reasons previously stated. [518:8]

* * * * *

IN THE SUPERIOR COURT OF
THE STATE OF CALIFORNIA IN AND FOR
THE COUNTY OF SAN DIEGO

Department 38 Honorable Laura W. Halgren, Judge

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. DAVID RILEY, Defendant.	CASE NO. SCD226240 TRIAL (PAGES 659 through 878)

REPORTER'S TRANSCRIPT
March 2, 2011

APPEARANCES:

For the People: BONNIE DUMANIS
District Attorney
By: JAMES SIMMONS
Deputy District Attorney
330 West Broadway
San Diego, California
92101

For the Defendant: EDWARD W. KINSEY
Attorney at Law
7760-H Fay Avenue,
Suite 303
La Jolla, California 92037

Reported By: DENISE CARRILLO, RPR,
CRR, CSR No. 9626
San Diego, California

* * * *

[DIRECT EXAMINATION OF
DUANE MICHAEL MALINOWSKI]

[BY MR. SIMMONS]:

[856:5]

Q. Now let's talk about August 22nd. Were you on duty on August 22nd of 2009?

A. Probably.

Q. And did you come into contact with Mr. Riley on that day after he was arrested with having two – a .45 and a .40 caliber gun?

A. I did. I was not working. It was a weekend morning, like a Saturday or Sunday morning. I got called at home again, stating that he had been arrested with some firearms, and I went downtown to speak to the officers and to interview Mr. Riley.

Q. Did you request that those firearms be submitted for DNA testing and ballistics?

A. Yes.

Q. Now, as far as – did you have the opportunity to go through a cell phone that was found on Mr. Riley?

A. I did.

Q. Did you see any – first of all, what is the cell phone number from that phone?

A. I would have to look at the report.

Q. Before you do that, let me ask you, did you record the number for the cell phone in your report?

A. I [sic] was recorded – there was a synopsis that was done that Detective Barnes and I both kind of prepared [857] together. I don't know if I have that with me or not today. I'd have to look.

Q. If it would refresh your recollection to review your report as to the number, please do so.

If I can help you – never mind.

A. I don't think I have that synopsis with me, unfortunately.

Q. The synopsis that you prepared along with Detective Barnes?

A. Correct.

Q. Would looking at a copy of that help refresh your recollection?

A. It would, yes. I believe that lists all the phone numbers that were pertinent.

Q. I will refer you to Page 2 of this four-page report, the third paragraph.

A. I got it.

Q. What was Mr. Riley's cell phone number?

A. (619) 634-4159.

Q. Did you see any videos or – excuse me – any photos in that cell phone of the red car which we're talking about?

A. I don't recall any photos. I think there were some photos found later on there. I didn't go through everything. But on one of the videos – I found some videos on there, and you can see a portion of that car in the video, like the back quarter panel portion of it.

Q. The photo you have in front of you, which is [858] People's Exhibit 2, I believe –

A. Yes.

Q. – Was that a photo you got from the cell phone?

A. This was one that was, I believe, on the cell phone, but when I was looking through it, I didn't see this. I was more interested in some of the videos that I was watching and some of the phone numbers.

Q. Did you actually look at other photos in that cell phone?

A. Yes.

(Whereupon, People's Exhibit No. 39, Photo of David Riley, showing hand signs, was marked for identification.)

(Whereupon, People's Exhibit No. 40, Photo of David Riley and Gerald Haynes, showing hand signs, was marked for identification.)

(Whereupon, People's Exhibit No. 41, Photo of David Riley and Gerald Haynes, Riley's arm

around Haynes' shoulder, was marked for identification.)

(Whereupon, People's Exhibit No. 28, photo of Ajon Webster, was marked for identification.)

BY MR. SIMMONS:

Q. I have a few I want to show you. I have what has been premarked for identification as People's Exhibits 39 through 41 and also have People's Exhibit 28 for [859] identification. Let's look at 39 through 41 first.

Looking at 39, do you recognize that photo?

A. Yes.

Q. What is it?

A. It's a photo of Mr. Riley standing in front of the car. It's at a different location, I believe on Altamar. I think that's the name of the street. He is doing a hand sign with his hands. He is making like an "L" with his thumb and index finger.

MR. SIMMONS: For the record, Your Honor, I am going to ask that these be received after he is done, but I am going to actually publish them when Detective Barnes comes in.

THE COURT: That's fine.

BY MR. SIMMONS:

Q. Let's go to the next photo, which is People's Exhibit 40 for identification. What is that?

A. It's another photo at that same location, out in front of the car. There is another – in the first photo, 39, there is a gentleman behind him, Mr. Haynes, and in this one, Mr. Haynes is standing next to Mr. Riley,

and they are doing a different hand sign with their hands.

Q. For the record, you put your right –

A. Basically, all my fingers extended to the left, with the thumb being up and the ring finger being tucked in.

Q. Let's go to the next photograph, which is People's Exhibit 41 for identification. What is that?

[860]

A. It's another picture of Mr. Haynes and Mr. Riley standing next to that vehicle. I think it's down on Altamar, like I said, in front of Mr. Haynes' house. Mr. Riley is doing that second hand sign where the ring finger is brought in, and then it looks like Mr. Haynes, with his right hand, is doing an "L," like a gun, basically.

Q. And let's go to the next photograph, which is People's Exhibit 28. Do you recognize the person in that photograph?

A. Yes, this is Mr. Webster. He is the gentleman that was in the green Camaro the day of the shooting.

MR. SIMMONS: I would ask that all of these be received, but I would only like to publish 28 at this time.

THE COURT: Any objection to receiving those items?

MR. KINSEY: None other than previously stated.

THE COURT: Subject to your other objection. So noted.

Those will be received, 28, 39, 40, and 41. And you may publish 28.

MR. SIMMONS: Thank you. [860:23]

* * * * *

IN THE SUPERIOR COURT OF
THE STATE OF CALIFORNIA IN AND FOR
THE COUNTY OF SAN DIEGO

Department 38 Honorable Laura W. Halgren, Judge

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. DAVID RILEY, Defendant.	CASE NO. SCD226240 TRIAL (PAGES 879 through 1070)

REPORTER'S TRANSCRIPT
March 3, 2011

APPEARANCES:

For the People: BONNIE DUMANIS
District Attorney
By: JAMES SIMMONS
Deputy District Attorney
330 West Broadway
San Diego, California
92101

For the Defendant: EDWARD W. KINSEY
Attorney at Law
7760-H Fay Avenue,
Suite 303
La Jolla, California 92037

Reported By: DENISE CARRILLO, RPR, CRR, CSR No. 9626
San Diego, California

* * * *

[DIRECT EXAMINATION OF SCOTT BARNES]

[BY MR. SIMMONS]:

[1045:15]

Q. Before we move on, I want to show you what has been premarked for identification as People's Exhibits 39 through 41. Why don't you take a look at those.

A. Okay.

Q. Do you recognize those?

A. I do.

Q. Who is the person depicted in People's Exhibit 39?

A. David Riley is – there are actually two people in there, but David Riley is standing in front of a red car, holding up a Lincoln gang sign.

Q. Who is the second person?

A. Behind the car, that is Gerald Haynes, who is also a Lincoln Park gang member.

[1046]

Q. Do you recognize the car in that photo?

A. I do.

Q. Whose car is that?

A. That's Mr. Riley's.

Q. And let's go to the next photo, which is People's Exhibit 40. Do you recognize what that is?

A. I do. That is David Riley and Gerald Haynes standing close to each other, both throwing up a Lincoln Park gang sign.

Q. I will post these in a second, and I'll have you explain which signs you are talking about.

Let's go to the next photograph, which is People's Exhibit 41 for identification. What is that?

A. Another photo of David Riley and Gerald Haynes standing together. Mr. Riley's arm is actually around Mr. Haynes, and they are both throwing up gang signs, Lincoln Park gang signs.

Q. You have seen these photos before, correct?

A. I have.

Q. And do you know where these photos came from?

A. Yeah. I don't remember where they came from. I have seen them several times, but I don't remember who took them.

Q. And the people in that photograph – is that Mr. Riley and Mr. Haynes in several of those photographs?

A. It is.

Q. All three?

A. All three.

[1047]

MR. SIMMONS: At this time the People would ask that People's 38 through 41 be received.

THE COURT: Thirty-eight is the map of the Lincoln Park area?

MR. SIMMONS: Yes.

THE COURT: Any objection?

MR. KINSEY: No, Your Honor.

THE COURT: That will be received.

(Whereupon, People's Exhibit No. 38 was received in evidence.)

THE COURT: Thirty-nine, 40, and 41 were received yesterday.

MR. SIMMONS: Yes.

THE COURT: So they are already in.

MR. SIMMONS: I'd ask that these be published at this time.

THE COURT: You may publish.

BY MR. SIMMONS:

Q. I want to first talk about 38. I want to post them all at the same time. Let me walk up to the screen.

Now I am pointing to the right of a green line. I believe it goes to – looks like 58th Street, is it?

A. Yes. 58th and Churchward.

Q. For the record, I am pointing to the middle of the map that borders 58th Street, and it goes down to the north, Imperial Avenue, and to the south, Division Street.

Are these the boundaries of Lincoln Park [1048] that you testified about?

A. Yes.

Q. And I believe you said to the west, to 805?

A. Yes.

Q. And to the north, Imperial Avenue?

A. Correct.

Q. And to the south, Division Street?

A. That's correct.

Q. Let me stay here. This is People's Exhibit 39. You said that is Mr. Riley in the front of the photograph?

A. That's correct.

Q. Now, looking at the photograph, Mr. Riley, with his left arm, is doing some kind of sign. You said it was a gang sign?

A. He is tossing up an "L" for Lincoln.

Q. And the male in the back of the red car, you said, is Mr. Haynes?

A. That's Gerald Haynes. Correct.

Q. Let's go to People's Exhibit 40. Which one is Mr. Riley in this photograph?

A. If you are looking at the picture, he is to the right.

Q. And what is Mr. Riley doing with his hands there, if you can tell us?

A. He is tossing up a Lincoln gang sign that stands [1049] for Lynch Mob, which is one of the clicks [sic] I named off earlier of the Lincoln Park street gang.

Q. And Mr. Haynes is to his left. Can you tell us what Mr. Haynes is doing with his hands.

A. He is doing the same thing.

Q. They are both throwing up Lynch Mob?

A. That's correct.

Q. And, finally, People's Exhibit 41. Mr. Riley is on the right of this photograph as well?

A. That's correct.

Q. And what is Mr. Riley doing with his hands?

A. Again, he is tossing up a Lincoln Park gang sign, Lynch Mob gang sign.

Q. And we see Mr. Haynes with his right hand – you said he is throwing a gang sign as well?

A. In that one, he is actually tossing up Lincoln Park, the "L" for Lincoln Park.

Q. Is Mr. Haynes younger or older than Mr. Riley?

A. He is younger than Mr. Riley.

Q. Do gang members – in the gang culture, is it typical to have a younger member of the gang come up under an older member?

A. It is.

Q. What is the reason for that?

A. Older gang members are always recruiting younger gang members to come up underneath them. There are strength in numbers. The more people you have in a street gang, the more fear that you can

produce, the stronger you [1050] are. It's the strength-in-number philosophy.

Q. And do you have an opinion as to whether Mr. Haynes is a Lincoln Park gang member?

A. I do.

Q. What is that opinion?

A. That he is a Lincoln Park street gang member.

Q. Have you seen any contacts or photos or videos, other than the three we just saw, connecting Mr. Riley and Mr. Haynes?

A. I have.

Q. And what are those?

A. Other than the photos, I have viewed a video on Mr. Riley's cell phone of Gerald Haynes street boxing with another Lincoln Park gang member named Cedric Black. Street boxing is something gang members do among themselves to fine-tune their fighting skills. And in that video, there are several things that are going on, but one is Gerald Haynes boxing with another Lincoln Park gang member, Cedric Black.

I believe you can also see – in one of the videos, you can see Mr. Riley's car. There is also another Lincoln Park gang member named Donte Haddock who is street boxing. They both take turns. He then is street boxing with Cedric Black, a Lincoln Park gang member.

Q. And during those videos, can you hear Mr. Riley's voice at all?

A. You can.

[1051]

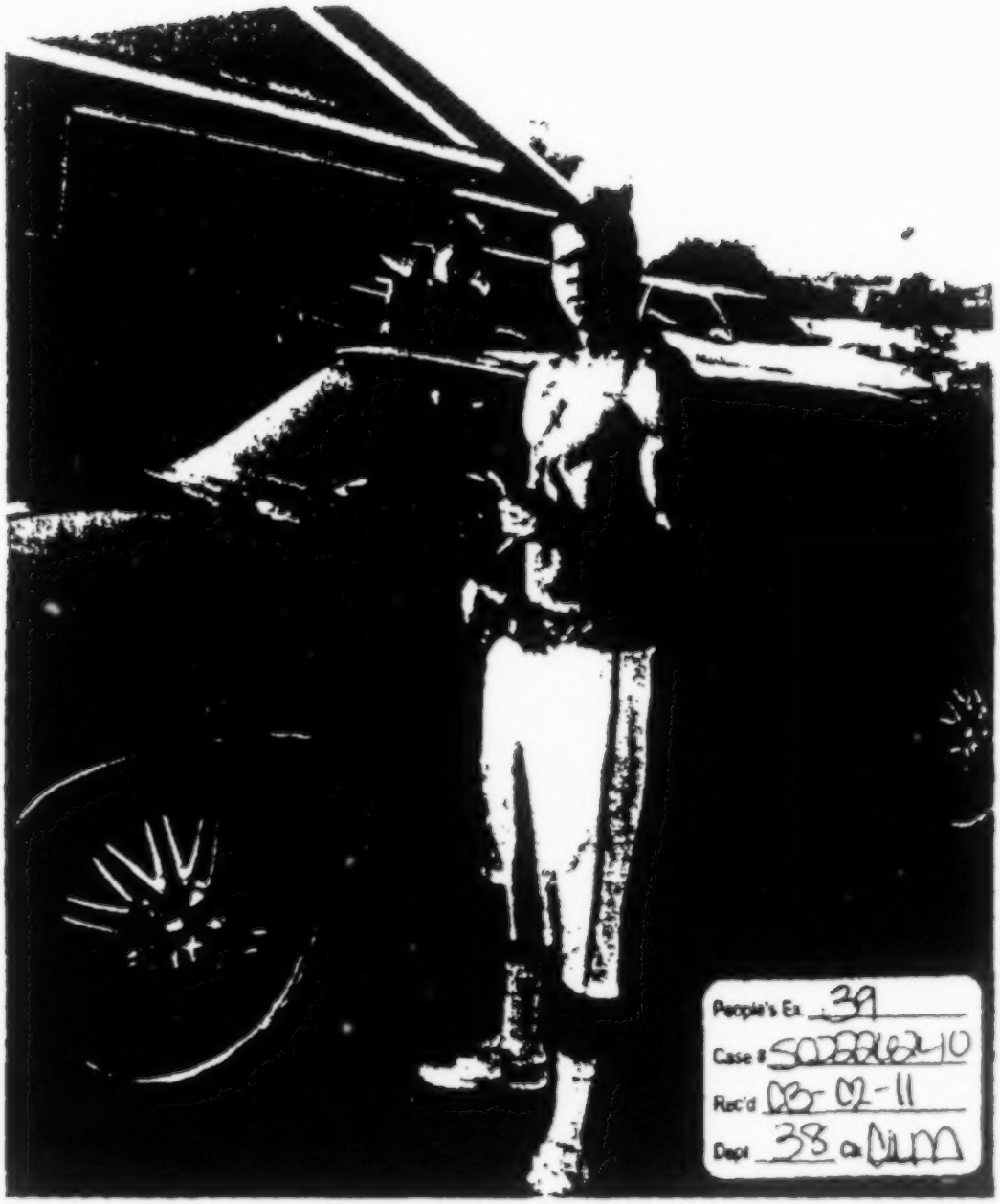
Q. And does he say anything during those videos that are gang-related?

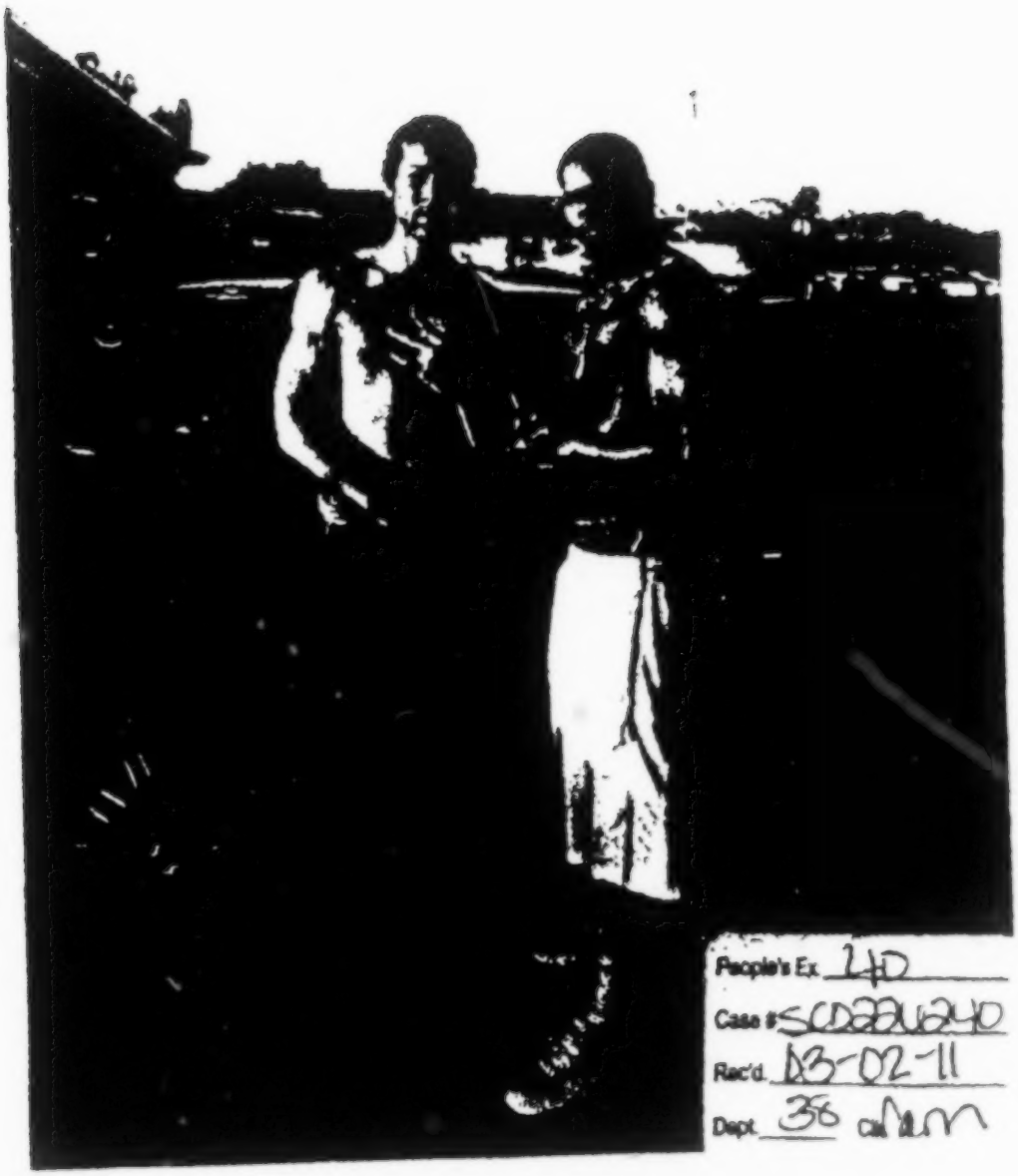
A. I believe he calls Gerald Haynes a "Little Bo" at one point. I would consider that gang-related.

Q. Based on the name "Little Bo," what would that mean to you?

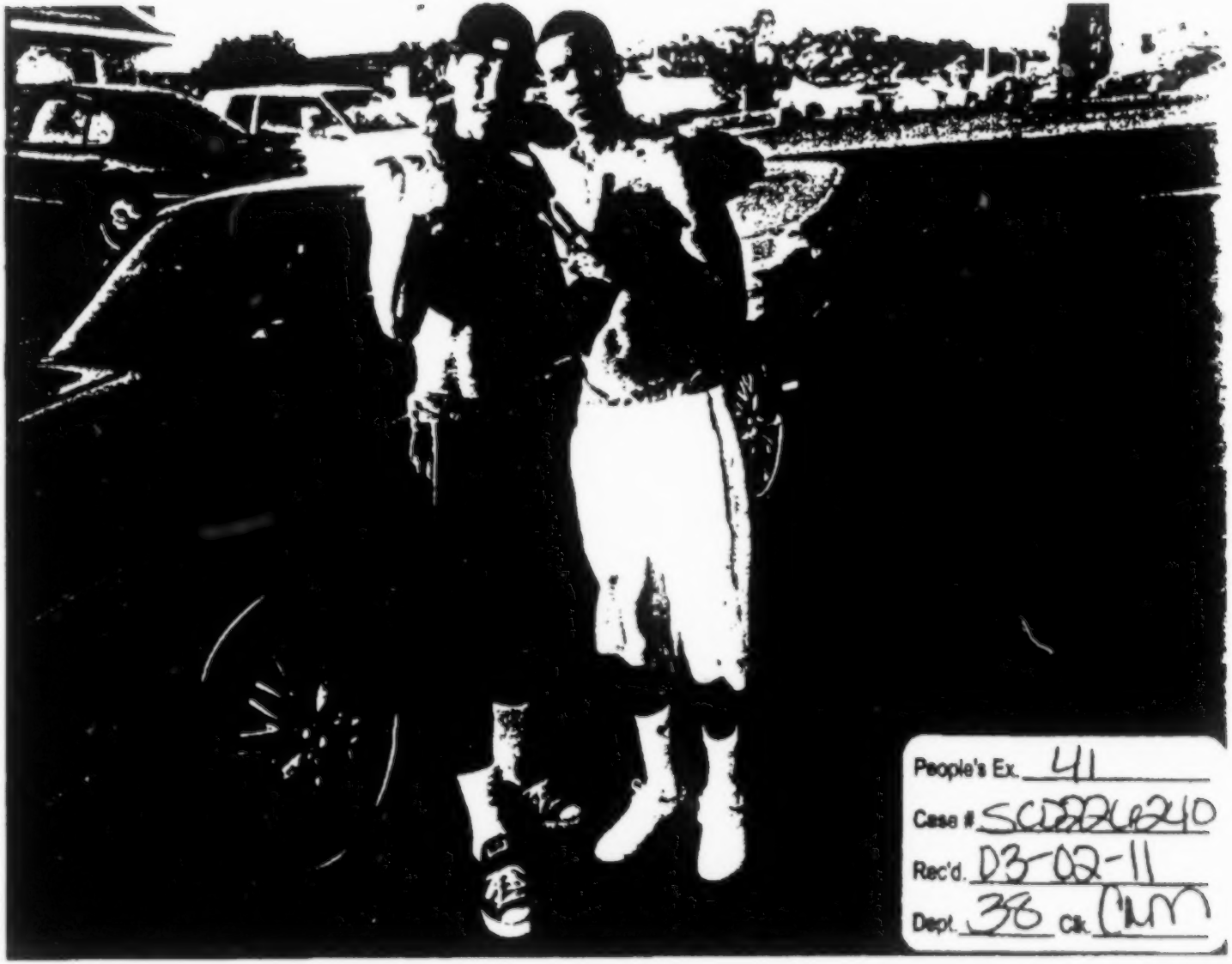
A. Well, if he is Dave Bo and he is calling someone Little Bo, who is younger than him, that's the one coming up underneath him. [1051:9]

* * * * *


People's Ex. 39
Case # SO22262210
Rec'd 03-02-11
Dept 38 on DLM



People's Ex. 14
Case # SCD221240
Rec'd 03-02-11
Dept. 36


People's Ex. 41
Case # SCD222624D
Rec'd. 03-02-11
Dept. 38 Clk. CM

PETITIONER'S BRIEF

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
MAR 3 - 2014
OFFICE OF THE CLERK

No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari
to the California Court of Appeal,
Fourth Appellate District

BRIEF FOR PETITIONER

Patrick Morgan Ford
LAW OFFICE OF PATRICK MORGAN FORD
1901 First Avenue
Suite 400
San Diego, CA 92101

Donald B. Ayer
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001

Jeffrey L. Fisher
Counsel of Record
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@law.stanford.edu

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

QUESTION PRESENTED

Whether evidence admitted at petitioner's trial (namely, certain digital photographs and videos) was obtained in a search of petitioner's cell phone that violated petitioner's Fourth Amendment rights.

TABLE OF CONTENTS

QUESTION PRESENTED i
TABLE OF AUTHORITIES iv
BRIEF FOR PETITIONER 1
OPINIONS BELOW 1
JURISDICTION 1
RELEVANT CONSTITUTIONAL PROVISION 1
INTRODUCTION 2
STATEMENT OF THE CASE 4
SUMMARY OF ARGUMENT 10
ARGUMENT 13
I. The Search Of The Digital Contents Of Petitioner's Smart Phone Exceeded The Bounds Of A Legitimate Search Incident To Arrest 13
A. The Search Was Unnecessary To Serve Any Legitimate Governmental Interest 15
1. Digital Data Does Not Threaten Officer Safety 16
2. Once Seized, It Is Unnecessary To Search A Smart Phone Without A Warrant To Preserve Evidence 20
B. The Degree of Intrusiveness Of The Search Of Petitioner's Phone Rendered The Search Unreasonable 24
1. Smart Phones Hold Extraordinary Amounts Of Sensitive Personal Information 26

2. Smart Phones Hold Information That Implicates First Amendment Concerns 31

C. Limiting Searches Of Smart Phones To Situations In Which Officers Believe Such Phones Contain Evidence Of The Crime Of Arrest Would Not Solve The Constitutional Problems Inherent In Such Searches 38

II. The Search Of Petitioner's Phone At The Stationhouse Was Too Remote From His Arrest To Qualify As A Search Incident To Arrest 44

CONCLUSION 53

TABLE OF AUTHORITIES

Page(s)

Cases

A Quantity of Copies of Books v. Kansas, 378 U.S. 205 (1964) 33

Abel v. United States, 362 U.S. 217 (1960) 49

Agnello v. United States, 269 U.S. 20 (1925) 45

Arizona v. Gant, 556 U.S. 332 (2009) .....*passim*

Arkansas v. Sanders, 442 U.S. 753 (1979) 20

Atwater v. City of Lago Vista, 532 U.S. 318 (2001) 3

Bailey v. United States, 133 S. Ct. 1031 (2013) 45

Boyd v. United States, 116 U.S. 616 (1886) .....*passim*

Cardwell v. Lewis, 417 U.S. 583 (1974) 39, 40, 47

Carroll v. United States, 267 U.S. 132 (1925) 39

Chambers v. Maroney, 399 U.S. 42 (1970) 46

Chimel v. California, 395 U.S. 752 (1969) .....*passim*

City of Indianapolis v. Edmond, 531 U.S. 32 (2000) 34

City of Ontario v. Quon, 560 U.S. 746 (2010) 37

Commonwealth v. Pierre, 893 N.E.2d 378 (Mass. App. Ct. 2008) 47

Cooper v. California, 386 U.S. 58 (1967) 50

D'Antorio v. State, 926 P.2d 1158 (Alaska 1996) 51

Diaz v. California, 132 S. Ct. 94 (2011) 9

Dyke v. Taylor Implement Mfg. Co., 391 U.S. 216 (1968) 46

Entick v. Carrington, (1765) 95 Eng. Rep. 807 (C.P), 19 How. St. Tr. 1029 ..... 32, 34

Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510 (2012) 19

Harris v. United States, 331 U.S. 145 (1947) 35

Illinois v. Lafayette, 462 U.S. 640 (1983) 50

Illinois v. McArthur, 531 U.S. 326 (2001) 20

Interstate Commerce Comm'n v. Brimson, 154 U.S. 447 (1894) 32

Katz v. United States, 389 U.S. 347 (1967) 14, 15

Knowles v. Iowa, 525 U.S. 113 (1998) 16

Kyllo v. United States, 533 U.S. 27 (2001) 13, 14

Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979) 33

Marcus v. Search Warrant, 367 U.S. 717 (1961) 32, 33

Maryland v. Garrison, 480 U.S. 79 (1987) 31

Maryland v. King, 133 S. Ct. 1958 (2013) 24, 25, 26, 28, 30

Missouri v. McNeely, 133 S. Ct. 1552 (2013) 20

NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958) 33

Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989) 30

New York v. Belton, 453 U.S. 454 (1981) 17, 19, 44

Newhard v. Borders, 649 F. Supp. 2d 440 (W.D. Va. 2009) 37

Pennsylvania v. Labron, 518 U.S. 938 (1996) 39

People v. Diaz, 244 P.3d 501 (Cal. 2011)) ..... *passim*

People v. McKay, 41 P.3d 59 (Cal. 2002) 2

People v. Redmond, 390 N.E.2d 1364 (Ill. App. Ct. 1979) 47

Preston v. United States, 376 U.S. 364 (1964) 44, 45, 46, 47

Roaden v. Kentucky, 413 U.S. 496 (1973) 17, 44

Shipley v. California, 395 U.S. 818 (1969) 44

Sibron v. New York, 392 U.S. 40 (1968) 17

South Dakota v. Opperman, 428 U.S. 364 (1976) 39, 51

Stanford v. Texas, 379 U.S. 476 (1965) 32, 33

State v. Davis, 742 P.2d 1356 (Ariz. Ct. App. 1987) 51

State v. Granville, ___ S.W.3d ___, 2014 WL 714730 (Tex. Crim. App. Feb. 26, 2014) 28, 29

State v. Isaac, 209 P.3d 765, No. 101,230, 2009 WL 1858754 (Kan. Ct. App. 2009) 44

State v. Murray, 605 A.2d 676 (N.H. 1992) 47

State v. Smith, 920 N.E.2d 949 (Ohio 2009) 8

Thornton v. United States, 541 U.S. 615 (2004) 16

Tobe v. City of Santa Ana, 892 P.2d 1145 (Cal. 1995) 2

United States v. $639,558 in U.S. Currency, 955 F.2d 712 (D.C. Cir. 1992) 47

United States v. Bennett, 409 F.2d 888 (2d Cir. 1969) 36

United States v. Butler, 904 F.2d 1482 (10th Cir. 1990) 47

United States v. Chadwick, 433 U.S. 1 (1977) ..*passim*

United States v. DiMarco, No. 12 CR 205(RPP), 2013 WL 444764 (S.D.N.Y. 2013) 44

United States v. Edwards, 415 U.S. 800 (1974) ..... *passim*

United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) 22

United States v. Gibson, No. CR 11-00734 WHA, 2012 WL 1123146 (N.D. Cal. 2012) 44

United States v. Jones, 132 S. Ct. 945 (2012) 14, 33, 41

United States v. Kirschenblatt, 16 F.2d 202 (2d Cir. 1926) 29, 35, 36

United States v. Lefkowitz, 285 U.S. 452 (1932) 30, 34, 35

United States v. Montalvo-Cruz, 662 F.2d 1285 (9th Cir. 1981) 47

United States v. Morales, 923 F.2d 621 (8th Cir. 1991) 47

United States v. Place, 462 U.S. 696 (1983) 20

United States v. Robinson, 414 U.S. 218 (1973) ..... *passim*

United States v. Robinson, 471 F.2d 1082 (D.C. Cir. 1972) (en banc) 18

United States v. Schleis, 582 F.2d 1166 (8th Cir. 1978) 47

United States v. Vasey, 834 F.2d 782 (9th Cir. 1987) 47

United States v. Wurie, 724 F.3d 255 (1st Cir. 2013) 25

United States v. Wurie,
728 F.3d 1 (1st Cir. 2013) ..... *passim*

United States v. Yockey, No. CR09-4023-MWB,
2009 WL 2400973 (N.D. Iowa 2009) 44

Vernonia Sch. Dist. 47J v. Acton,
515 U.S. 646 (1995) 14, 15, 24

Weems v. United States, 217 U.S. 349 (1910) 14

Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (C.P.),
19 How. St. Tr. 1153 32

Williams v. District of Columbia,
439 F. Supp. 2d 34 (D.D.C. 2006) 20

Wyoming v. Houghton, 526 U.S. 295 (1999) 25, 39

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) 33

Constitutional Provisions

U.S. Const., amend. I 11, 25, 31, 33

U.S. Const., amend. IV ..... *passim*

Statutes

18 U.S.C. §§ 2511-2522 52

18 U.S.C. § 2701 52

18 U.S.C. § 2703(a) 52

28 U.S.C. § 1257(a) 1

Cal. Penal Code § 186.22(b)(4)(B) 9

Cal. Penal Code § 246 9

Cal. Penal Code § 12025(a)(1) 43

Cal. Penal Code § 12031(a)(1) 43

Cal. Penal Code § 25400(a)(1) 43

Cal. Penal Code § 25850(a)(1) 43

Other Authorities

Apple, *Apple – iPhone 5s – Technical Specifications* 42

Apple, *iCloud Photo Sharing* 53

Brady, Surell, *Arrests Without Prosecution and the Fourth Amendment*, 59 Md. L. Rev. 1 (2000) 2

Brown, Edmund G., Governor, Letter to Members of California State Senate (Oct. 9, 2011) 9

Cal. Dep't of Justice, Bureau of Forensic Servs., Physical Evidence Bulletin: Digital Evidence Collection – Mobile Devices (2011) 23

Dep't of Justice Computer Crime and Intellectual Prop. Section, Cybercrime Lab, Awareness Brief: Find My iPhone (2009) 23

Digital Photos Taken by Americans, Nat'l Geographic, April 2012 41

Dripps, Donald A., *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49 (2013) 34, 36

Fed. Bureau of Investigation, Crime in the United States (2012) 2

Gershowitz, Adam M., *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 Wm. & Mary Bill Rts. J. 601 (2013) 23, 24

Harris, Kamala D., Cal. Dep't of Justice, Crime in California (2012) 2

LaFave, Wayne R., Search and Seizure (5th ed. 2012) 3

Miller, Christa, et al., *What's in an App? Extracting and Examining Mobile Device App Data*, Evidence Tech. Mag. (Nov.– Dec. 2013) 24

N.Y. Div. of Criminal Justice Servs., Adult Arrests: 2003-2012 (2013) 2

Orso, Matthew E., *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L. Rev. 183 (2010) 27

Samsung, *Samsung Galaxy S4 – Life Companion* 42

Samsung, *Samsung Instinct Touchscreen Cell Phone* 5, 22

Samsung, Samsung Instinct User Guide (2008) 22, 27, 41

Schnapper, Eric, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869 (1985) 34, 36

Shankland, Stephen, *How Google Is Becoming an Extension of Your Mind*, CNET (July 16, 2012) 27

Wood, Molly, *Narcissist's Dream: Selfie-Friendly Phone*, N.Y. Times, Feb. 6, 2014 41

BRIEF FOR PETITIONER

Petitioner David Leon Riley respectfully requests that this Court reverse the judgment of the California Court of Appeal.

OPINIONS BELOW

The opinion of the California Court of Appeal (Pet. App. 1a) is unpublished but can be found at 2013 WL 475242. The order of the California Supreme Court denying review (Pet. App. 24a) is unpublished. The relevant trial court proceedings and order are unpublished.

JURISDICTION

The California Supreme Court denied review on May 1, 2013. Pet. App. 24a. This Court granted a writ of certiorari on January 17, 2014. 134 S. Ct. 999 (2014). This Court has jurisdiction pursuant to 28 U.S.C. § 1257(a).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment states in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."

INTRODUCTION

Every day across the country, thousands of people are arrested – a reality that results in over twelve million people being arrested each year,[1] a majority of whom are never convicted of any crime. Surell Brady, *Arrests Without Prosecution and the Fourth Amendment*, 59 Md. L. Rev. 1, 3 (2000). While some of these arrests arise from felony investigations, the vast majority are for alleged misdemeanors such as driving under the influence, simple assault, or petty theft. In California, for example, about two-thirds of adult arrests are for misdemeanors;[2] in New York, almost three-fourths are for misdemeanors.[3]

What is more, in California as in most other states, the police may – and sometimes do – arrest people for traffic and other "fine only" infractions such as jaywalking, littering, or riding a bicycle the wrong direction on a residential street. *People v. McKay*, 41 P.3d 59, 62-63 (Cal. 2002); *Tobe v. City of*

---

[1] Fed. Bureau of Investigation, Crime in the United States 2012 tbl.29 (2012), *available at* http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/tables/29tabledatadecpdf.

[2] Kamala D. Harris, Cal. Dep't of Justice, Crime in California 2 (2012), *available at* http://oag.ca.gov/sites/all/files/agweb/pdfs/cjsc/publications/candd/cd12/cd12.pdf. By far, the most common offense of arrest is driving under the influence. Over 15% of total arrests in recent years (about 200,000 per year) are for DUI. *Id.* at 19 tbl.18, 29 tbl.26.

[3] N.Y. Div. of Criminal Justice Servs., Adult Arrests: 2003-2012 (2013), *available at* http://www.criminaljustice.ny.gov/crimnet/ojsa/arrests/NewYorkState.pdf.

Santa Ana, 892 P.2d 1145, 1178 (Cal. 1995); *see also Atwater v. City of Lago Vista*, 532 U.S. 318, 354-55 (2001). Indeed, given that "very few drivers can traverse any appreciable distance without violating some traffic regulation, . . . it is apparent that virtually everyone who ventures out onto the public streets and highways may then, with little effort by the police, be placed in a position where he is subject to a full search." 3 Wayne R. LaFave, Search and Seizure § 5.2(e), at 156 (5th ed. 2012) (internal quotation marks and citation omitted).

According to the California Supreme Court, every time the police effectuate one of these arrests and searches, officers may not only seize and secure any smart phone the arrestee is carrying but also may rummage through the digital contents of the device. *See People v. Diaz*, 244 P.3d 501 (Cal. 2011) (reprinted at Pet. App. 25a-65a). Furthermore, the police may undertake such warrantless examinations not only briefly at the scene of arrest but also later at the police station after booking the arrestee. *Diaz*, Pet. App. 33a.

This case concerns whether granting such a new police entitlement comports with the Fourth Amendment. The stakes are high: Americans use smart phones to generate and store a vast array of their most sensitive thoughts, communications and expressive material. Because the core purpose of the Fourth Amendment has always been to safeguard such personal and professional information from exploratory searches, this Court should hold that even when officers seize smart phones incident to lawful arrests, they may not search the phones' digital contents without first obtaining a warrant.

STATEMENT OF THE CASE

1. Early in the morning on August 22, 2009, the police pulled over petitioner David Riley, a local college student, who was driving his Lexus near his home in the Lincoln Park neighborhood of San Diego. The officer who initiated the stop, Charles Dunnigan, told petitioner that he had pulled him over for having expired tags. Pet. App. 3a, 5a. Officer Dunnigan soon learned that petitioner was driving with a suspended license. The officer thus decided to impound petitioner's car.

At the inception of an impound, San Diego Police Department policy requires officers to conduct an inventory search of the vehicle in order to document its contents. Pet. App. 5a. Officer Dunnigan called in another officer to assist with this task. J.A. 5-6. During the inventory search, the officers looked under the car's hood and discovered two firearms. Pet. App. 3a, 6a. Based on this discovery, Officer Dunnigan placed petitioner under arrest for carrying concealed and loaded weapons. *Id.* 6a.

During the arrest, Officer Dunnigan seized petitioner's cell phone from his pants pocket. Pet. App. 5a, 15a.[4] According to a "phone examination report" that the State provided during discovery, the

---

[4] Some testimony presented at trial suggested that petitioner's phone might have been sitting on the seat of his car instead of in his pocket at the time of arrest. Pet. App. 15a. But the trial court found that "the cell phone . . . was on [Riley's] person at the time of the arrest," and the California Court of Appeal treated that finding as binding for purposes of appeal. *Id.* Accordingly, petitioner proceeds here on the basis of that finding as well.

phone was a Samsung SPH-M800 Instinct "smart phone." This touch-screen device – designed to compete with Apple's original iPhone and the iPhone 3G – is capable of accessing the internet, capturing and storing photos and videos, providing and storing GPS location information, and capturing and storing both voice and text messages, among other features. *Samsung Instinct Touchscreen Cell Phone: Features*, Samsung, http://www.samsung.com/us/mobile/cell-phones/SPH-M800ZKASPR-features.

After seizing petitioner's phone, officers performed a two-stage warrantless search of its digital contents. First, Officer Dunnigan scrolled through the phone's "text entries" at the scene. BIO 1, 12. He noticed that some words (apparently in text messages and the phone's contacts list) normally beginning with the letter "K" were preceded by the letter "C." *Id.*; Pet. App. 6a; J.A. 8. Having already noticed other indications (such as the colors on petitioner's key chain) that petitioner might be connected with a criminal gang, Officer Dunnigan believed that the "CK" prefix referred to "Crip Killers," a slang term for members of a gang known as the "Bloods." J.A. 8.

The second search of petitioner's phone took place "about two hours later" at the police station. BIO 2. After the arresting officers booked petitioner, Detective Duane Malinowski, a detective specializing in gang investigations, took him upstairs to an interview room and attempted to interrogate him. Petitioner was nonresponsive. Detective Malinowski then released petitioner back to the arresting officers and retrieved the property they had seized from him

at the time of arrest, including his smart phone. J.A. 15-16.

As Detective Malinowski later explained, he "went through" and downloaded "a lot of stuff" on the phone "looking for evidence." J.A. 11, 14, 20. It is unclear how many different digital files on the phone Detective Malinowski reviewed. But at a minimum, he looked through the digital files containing photographs, watched numerous videos, and reviewed the phone's collection of phone numbers. *Id.* 30-31. "[O]ne of the things that caught [his] eye" were videos of "street boxing" – that is, friends sparring with each other with bare hands, taking care not to really hurt each other. *Id.* 11, 17. Petitioner was not among those street boxing in the videos, but Detective Malinowski believed that he could hear him in the background shouting gang-like terms, such as "Come on Lincoln" and "Get him blood." *Id.* 13. Detective Malinowski also found a few photos of petitioner with another young man, both allegedly making hand signals indicating gang membership. In the background of these photos, reproduced at J.A. 42-44, Detective Malinowski noticed a red Oldsmobile that the police suspected had been involved in a prior shooting.

In that incident, three individuals fired several shots at a passing car before reportedly fleeing in a red Oldsmobile. The police believed the shooting was gang related. After finding the photos on petitioner's phone indicating that he owned a red Oldsmobile and that he was connected to gang activity, and after ballistics testing suggested that the firearms seized during petitioner's traffic stop were used in the

shooting incident, law enforcement came to believe that petitioner had been involved in that altercation.

2. The State ultimately charged petitioner and two others with shooting at an occupied vehicle, assault with a semi-automatic firearm, and attempted murder.[5] The State also alleged that petitioner committed these crimes for the benefit of a criminal street gang – an allegation that not only rendered the potentially inflammatory evidence of petitioner's alleged gang membership admissible (and, indeed, highly relevant) at trial, but also exposed him under California law to a significantly enhanced sentence. The two co-defendants eventually pleaded guilty to involvement in the crime, but petitioner insisted on his innocence.

Prior to trial, petitioner moved to suppress all of the evidence the police had obtained during the searches of his cell phone. Tr. at 269-70. As is pertinent here, petitioner argued that the search of his cell phone violated the Fourth Amendment because it was performed without a warrant and without any exigency otherwise justifying the search. *Id.* The trial judge rejected this argument, ruling that the searches were legitimate searches incident to arrest. Pet. App. 7a-8a. The trial ended in a hung jury, but the State elected to retry petitioner.

---

[5] The State separately charged petitioner in conjunction with the traffic stop with carrying a concealed firearm in a vehicle, carrying a loaded firearm, and receiving stolen property. Petitioner pleaded guilty to all three charges and was sentenced to four years in prison. Those convictions are not at issue here.

During the second trial (as at the first), none of the State's four eyewitnesses could identify petitioner as one of the shooters. The State, therefore, relied on circumstantial evidence to connect petitioner to the crime. Among other things, the State again sought to show the jury the photos of petitioner posing in front of the Oldsmobile with one of the co-defendants. J.A. 35-40, 42-44. In addition, the State sought to rely on the videos from petitioner's cell phone showing street boxing fights involving both co-defendants, in which petitioner could be heard in the background encouraging the co-defendants and shouting supposedly gang-related comments. *Id.* 40-41.

The trial court again ruled the evidence was admissible, J.A. 26 (ruling); *id.* 30-31, 40-41 (introduction of evidence), this time basing its ruling on the California Supreme Court's decision in *People v. Diaz*, 244 P.3d 501 (Cal. 2011). In that decision – which was announced between the two trials here, and which is reproduced at Pet. App. 25a-65a – the California Supreme Court held by a 5-2 vote that the Fourth Amendment's search-incident-to-arrest doctrine permits the police to conduct a full exploratory search of a cell phone (even some time later at the stationhouse) whenever the phone is immediately associated with the arrestee's person at the time of the arrest. *Diaz*, Pet. App. 33a-34a. The majority acknowledged that the Ohio Supreme Court had reached a contrary conclusion. *Id.* 47a n.17. That court reasoned that "modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object" that might otherwise be seized incident to arrest. *State v. Smith*, 920 N.E.2d 949, 954 (Ohio 2009). But the California Supreme Court insisted that only this

Court has the power to consider how its jurisprudence dealing with physical containers should apply to the "modern technology" of the digital age. *Diaz*, Pet. App. 47a.[6]

The jury ultimately convicted petitioner on all three charges. Pursuant to California law, the trial court activated only petitioner's sentence for the conviction that carried the longest sentence, shooting at an occupied vehicle, and stayed petitioner's sentences for the two other convictions. Without the gang enhancement, this crime is punishable by a maximum of seven years in prison. Cal. Penal Code § 246. With the enhancement, however, petitioner's conviction for shooting at an occupied vehicle required the court to sentence him to fifteen years to life in prison. Pet. App. 1a; *see also* Cal. Penal Code § 186.22(b)(4)(B).

---

[6] Mr. Diaz filed a petition for a writ of certiorari challenging the California Supreme Court's holding. Shortly thereafter, the California Legislature overwhelmingly passed a bill requiring the police to obtain a warrant before searching the contents of any "'portable electronic devices,' including cellular telephones." Supp. Br. to Br. in Opp. 1, *Diaz v. California*, 132 S. Ct. 94 (2011) (No. 10-1231), 2011 WL 4366007, at *1 (describing Senate Bill 914 (2011)). After the State brought the bill to this Court's attention, *see id.*, the Court denied review. 132 S. Ct. 94 (2011). One week later, California Governor Jerry Brown vetoed the state legislature's bill, stating that the "courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections." Letter from Edmund G. Brown Jr., Governor, to Members of the California State Senate (Oct. 9, 2011), *available at* http://gov.ca.gov/docs/SB_914_Veto_Message.pdf.

3. The California Court of Appeal affirmed the judgment. As is relevant here, the court held that "*Diaz* controls the present case" because the cell phone was "immediately associated with [petitioner's] person" at the time of his arrest. Pet. App. 15a (internal quotation marks and citation omitted).

4. Petitioner sought discretionary review in the California Supreme Court. As is pertinent here, he renewed his argument that the warrantless searches of his cell phone violated the Fourth Amendment. Pet. for Review at 13-20. The California Supreme Court denied review without comment. Pet. App. 24a.

SUMMARY OF ARGUMENT

The warrantless search of the digital contents of petitioner's smart phone violated the Fourth Amendment.

I. Searching the digital contents of a smart phone furthers neither of the governmental interests that justifies searches incident to arrest and impinges upon personal privacy to an unprecedented degree.

A. Police officers may conduct warrantless searches incident to arrest in order to search for weapons and to prevent the destruction of evidence. Neither of those concerns, however, is implicated here. Unlike physical items inside of a container, the digital contents of a smart phone are categorically incapable of threatening officer safety. And once the police have seized and secured a smart phone, there is no risk that the arrestee might destroy or alter its digital contents. Nor should there be any danger that a third party might do so; so long as the police prevent the phone from receiving a signal – for example, by placing it into a Faraday bag – the

digital contents of the device will remain frozen while the police decide whether to seek a warrant.

B. Searching text, photo, and video files within smart phones – as the police did here – severely impinges upon personal privacy. Such files hold exponentially greater amounts and types of sensitive personal information than any physical item an arrestee could carry on his person. Furthermore, much of that information implicates First Amendment concerns, such as free expression, private communication, and associational interests.

Indeed, subjecting smart phones seized at the time of arrest to exploratory searches at the whim of police officers would strike at the heart of the Fourth Amendment's fundamental concerns. The Framers incorporated the prohibition against unreasonable searches into the Bill of Rights primarily in response to the odious colonial-era practice of executing general warrants – warrants that enabled officers to rummage though people's homes and offices for whatever incriminating items they might find. Such searches were deemed particularly problematic when directed at people's "private papers" or other expressive documents.

Searching through a smart phone's text, photo, and video files would be the modern equivalent of such a general search. Before the development of smart phones, people kept the information stored on such devices – if it existed in tangible form at all – only in the most private recesses of their homes or offices, safely beyond the reach of any search that might occur incident to arrest. The information on smart phones is also profoundly expressive. It reveals the thoughts, wonders, and concerns of a

phone's owner – as well as of those with whom the owner has interacted in various ways. The protection the Fourth Amendment has always afforded to such writings and other expression should not evaporate – more than two hundred years after the Founding – simply because that information can now be reduced to electronic charges in a computer chip and carried in one's pocket.

C. Limiting searches of smart phones to situations where officers have a reasonable belief that such phones contain evidence of the crime of arrest would not solve the constitutional problems inherent in such searches. The reasonable-belief exception applies only in the unique context of automobile searches. Even if this Court were open to the possibility of extending that exception to other kinds of searches incident to arrest, the exception would be especially ill-suited to smart phones. Precisely because the digital contents of such devices contain virtually limitless amounts of information concerning people's daily activities and personal connections, an officer could almost always claim that he reasonably believed that he might find relevant evidence *somewhere* in a phone. Incessant litigation would ensue, and the exception, for all practical purposes, would swallow the rule.

II. Even if police officers could generally search the digital contents of smart phones seized during arrests, the search of petitioner's phone at the stationhouse still violated the Fourth Amendment because it was not truly "incident" to arrest. The search-incident-to-arrest doctrine condones warrantless searches only when performed substantially contemporaneous with the arrest and in

the immediate vicinity of the arrest. The search here satisfied neither requirement. It was conducted some two hours after petitioner's arrest and after he was booked at the stationhouse. Under these circumstances, there can be no doubt that the police had ample ability to seek a warrant before examining material on petitioner's smart phone. Their failure to do so rendered the search unreasonable.

ARGUMENT

I. The Search Of The Digital Contents Of Petitioner's Smart Phone Exceeded The Bounds Of A Legitimate Search Incident To Arrest.

In the decision that dictated the outcome below, the California Supreme Court asserted that "binding precedent" from the pre-digital age left it no choice but to treat searches of smart phones seized at the time of arrests identically to searches of purely physical objects. *People v. Diaz*, 244 P.3d 501, 511 (Cal. 2011) (reprinted at Pet. App. 25a, 47a); *see also id.* 51a (Kennard, acting C.J., concurring) (agreeing with the majority's approval of unrestricted cell phone searches "[u]nder the compulsion of directly applicable United States Supreme Court precedent").

But as this Court has repeatedly noted, "it would be foolish" to contend that the Fourth Amendment cannot take account of "the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). When a modern innovation gives law enforcement the ability to obtain personal information formerly beyond its reach, that "practical" reality requires this Court to assess the legality of the police practice at issue not only in light of prior case law but also, more generally, in terms of the timeless concerns

underlying the Fourth Amendment. *United States v. Jones*, 132 S. Ct. 945, 963-64 (2012) (Alito, J., concurring in the judgment) (GPS technology); *see also id.* at 955-57 (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 33-34 (infrared imaging); *Katz v. United States*, 389 U.S. 347, 352-53 (1967) (listening in on telephone calls). "Under any other [approach] a constitution would indeed be as easy of application as it would be deficient in efficacy and power. Its general principles would have little value and be converted by precedent into impotent and lifeless formulas." *Weems v. United States*, 217 U.S. 349, 373 (1910).

Put another way, this Court must remain ever alert to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. That obligation requires this Court to judge the legality of warrantless searches of a sort that the Framers could not have contemplated and that this Court has never considered against the traditional Fourth Amendment inquiries into (A) whether the searches further any legitimate governmental interest; and (B) the degree to which such searches impinge upon personal privacy. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995). Law developed with only physical objects in mind cannot be woodenly applied to digital files containing virtually limitless amounts of information – especially when most of that information would formerly have been stored in places, such as one's home, that were safe from government intrusion without a warrant.

For the reasons described below, warrantless searches of smart phones fail to further any legitimate law enforcement interest related to effectuating arrests. Such searches also impinge upon personal privacy to an unprecedented degree. Consequently, the Fourth Amendment's search-incident-to-arrest doctrine should not countenance such warrantless searches.

A. The Search Was Unnecessary To Serve Any Legitimate Governmental Interest.

"[E]very case addressing the reasonableness of a warrantless search [begins] with the basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions.'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357); *see also Acton*, 515 U.S. at 653 ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant."). "Among the exceptions to the warrant requirement is a search incident to a lawful arrest." *Gant*, 556 U.S. at 338.

This Court's modern search-incident-to-arrest jurisprudence emanates from *Chimel v. California*, 395 U.S. 752, 762-63 (1969), and *United States v. Robinson*, 414 U.S. 218, 234 (1973). In those cases, this Court explained that police officers may search an arrestee's person and the immediate vicinity in order to further two governmental interests: (1) to identify and "remove any weapons that the [arrestee] might seek to use in order to resist arrest or effect his

escape" and (2) to "seize any evidence on the arrestee's person in order to prevent its concealment or destruction." *Chimel*, 395 U.S. at 762-63; *see also Robinson*, 414 U.S. at 234 ("The justification or reason for the authority to search incident to a lawful arrest" rests upon "the need to disarm the suspect" and "the need to preserve evidence on his person.").

At the same time, this Court has stressed that "conducting a *Chimel* search is not the Government's right; it is an exception – justified by necessity." *Thornton v. United States*, 541 U.S. 615, 627 (2004) (Scalia, J., concurring in the judgment). When "there is no possibility" that the arrestee could gain access to a weapon or destroy evidence, "both justifications for the search-incident-to-arrest exception are absent and the rule does not apply." *Gant*, 556 U.S. at 339; *see also Knowles v. Iowa*, 525 U.S. 113, 118-19 (1998) (refusing to extend the search-incident-to-arrest doctrine to the issuances of citations because "the concern for officer safety is not present to the same extent and the concern for destruction or loss of evidence is not present at all").

Such is the case here: The digital contents of a smart phone cannot threaten officer safety, and there is no need to search such data to protect against the destruction of evidence.

1. Digital Data Does Not Threaten Officer Safety.

Once police seize a smart phone and have it securely in their possession, it is perfectly reasonable for officers to inspect the physical components of the phone (including any protective cover or case) to ensure that it does not pose a safety threat. But once that task is complete, there is no need to examine the

phone's *digital* contents – a series of ones and zeros stored electronically on computer chips – to protect against the arrestee resisting arrest or escaping.

In its decision in *Diaz* the California Supreme Court never disputed this reality. But it deemed it immaterial. Quoting language from this Court's opinion in *Robinson*, the California Supreme Court reasoned that when the police seize property from the person of an arrestee, "[i]t is the fact of the lawful arrest" – not any safety or other concern – "which establishes the authority to search." *Diaz*, Pet. App. 30a (quoting *Robinson*, 414 U.S. at 235).

This Court has cautioned, however, that the precedential force of any given Fourth Amendment decision depends on "the concrete factual context of the individual case." *Sibron v. New York*, 392 U.S. 40, 59 (1968); *see also Roaden v. Kentucky*, 413 U.S. 496, 501 (1973) ("A seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material."). In *Gant*, for instance, the State of Arizona argued – based on categorical-sounding language in this Court's decision in *New York v. Belton*, 453 U.S. 454 (1981) – that the Fourth Amendment permitted the police to search an arrestee's vehicle incident to arrest "even if there [were] no possibility the arrestee could gain access to the vehicle at the time of the search." *Gant*, 556 U.S. at 341. This Court rejected the argument, explaining that even though *Belton* could be read in that manner, the case had to be understood in the setting in which it arose, involving the exigency of "a single officer confronted with four unsecured arrestees." *Gant*, 556 U.S. at 344. Any other reading would have

"untether[ed] the rule [of *Belton*] from the justifications underlying the *Chimel* exception." *Gant*, 556 U.S. at 343.

The California Supreme Court made the same mistake here that the State of Arizona made in *Gant*. In *Robinson*, this Court upheld a search incident to arrest of an arrestee's person, which included an officer's inspection of a crumpled cigarette package found in the arrestee's shirt pocket. 414 U.S. at 235-36. Once the officer seized the package from the arrestee, there was no risk that any evidence inside could be destroyed. But, as the government explained and the dissenting judges in the court of appeals noted, "further inspection of the package was still justifiable as a protective measure" because the arrestee was standing immediately in front of the officer and the package might have contained "a razor blade," "live bullets," or even a pin. *United States v. Robinson*, 471 F.2d 1082, 1118 (D.C. Cir. 1972) (en banc) (Wilkey, C.J., dissenting); *see also* Br. for United States at 9-11, *Robinson*, 414 U.S. 218 (No. 72-936) (arguing that search of cigarette package was "justified by the inherent dangers to the safety to police" and that "the potential for danger was not abated until [the officer] examined it and discovered, not a weapon, but heroin").

Robinson thus presented no occasion to sever the search-incident-to-arrest doctrine forevermore from its conceptual underpinnings. Rather, that decision rested on the understanding that officers must make "quick ad hoc judgment[s]" when arresting people. *Robinson*, 414 U.S. at 235. And some chance – however small – always exists that an arrestee's body or a container of physical items taken from his person

might hold a weapon or device that could be used to effectuate an escape. *Id.*; *see also Florence v. Bd. of Chosen Freeholders*, 132 S. Ct. 1510, 1519 (2012) (observing that the human body can "conceal[] knives, scissors, razor blades, glass shards, and other prohibited items"); *United States v. Edwards*, 415 U.S. 800, 805 (1974) (noting that "at the time and place of the arrest" police officers may seize and examine arrestee's clothing). That being so, it would be unfair for courts to engage in "case-by-case adjudication" to determine "the probability in a particular arrest" that an arrestee or container on his person poses such a threat. *Robinson*, 414 U.S. at 234. Insofar as the physical universe is concerned, "the fact of custodial arrest [itself] gives rise to the authority to search." *Id.* at 236.

There is zero chance, however, that the digital contents of a smart phone can threaten officer safety. Unlike an arrestee's body or objects that this Court has characterized as "container[s]" – that is, "object[s] capable of holding another object" like a pin or razor blade, *Belton*, 453 U.S. at 460 n.4 – a smart phone does not hold any physical objects at all. It simply stores digital data, something that is plainly and categorically incapable of posing a danger to officers. In this situation, the teaching of *Gant* is that once the arrestee and the smart phone are securely in police custody, *Chimel*'s safety rationale "does not apply." 556 U.S. at 339.[7]

---

[7] The facts of *Robinson* also differ from the situation here in another respect. The government explained at oral argument in the case that if there had been nothing problematic inside the cigarette package, the officer would have immediately "given it

2. Once Seized, It Is Unnecessary To Search A Smart Phone Without A Warrant To Preserve Evidence.

Nor is it necessary to rummage through a smart phone's digital contents without seeking a warrant in order to prevent the destruction of evidence. It is hornbook law that the Fourth Amendment permits officers to secure spaces and seize items "where needed to preserve evidence until police could obtain a warrant." *Illinois v. McArthur*, 531 U.S. 326, 334 (2001) (home); *see also United States v. Place*, 462 U.S. 696, 706 (1983) (luggage); *Arkansas v. Sanders*, 442 U.S. 753, 766 (1979) (containers inside a car). And police officers can now obtain warrants in a matter of hours and sometimes minutes. *Missouri v. McNeely*, 133 S. Ct. 1552, 1562-63 (2013). Thus, the search-incident-to-arrest doctrine permits searching an item to preserve evidence only when a seizure alone is "[in]sufficient to guard against any risk that evidence might be lost" during the hours or minutes necessary to obtain a warrant. *United States v. Chadwick*, 433 U.S. 1, 13 (1977).

---

back" to the arrestee. Oral Arg. at 26:20, *Robinson*, 414 U.S. 218 (No. 72-936) *available at* http://www.oyez.org/cases/1970-1979/1973/1973_72_936; *see also Robinson*, 414 U.S. at 259 n.7 (Marshall, J., dissenting) (noting this explanation). (After all, the case arose in the early 1970s, when people carried cigarettes everywhere, including inside jails. *See, e.g., Williams v. District of Columbia*, 439 F. Supp. 2d 34, 38 (D.D.C. 2006) (noting the D.C. jail allowed inmates to smoke until 1992).) An officer in the situation here would never return a smart phone and allow the arrestee to take it with him into jail.

In *Chadwick*, for instance, this Court held that the search-incident-to-arrest doctrine did not allow officers to inspect the contents of a footlocker seized from an arrestee. Once it was clear that the officers had "exclusive control" over the footlocker and "there [was] no longer any danger that the arrestee might gain access to the property," it was "unreasonable to undertake the additional and greater intrusion of a search without a warrant." 433 U.S. at 13, 15. Likewise, in *Gant* this Court held that the *Chimel* doctrine "does not authorize a vehicle search incident to a recent occupant's arrest after the arrestee has been secured and cannot access the interior of the vehicle." 556 U.S. at 335.

These precedents apply with full force here. Once the police have exclusive control over a smart phone and have secured it beyond an arrestee's grab area, there is no legitimate concern that the arrestee could alter or destroy the phone's digital contents.

Faced with this actuality, the federal government offers an alternative basis to justify searching a smart phone to preserve evidence. The government contends that "[u]nlike [cigarette packages or clothes], which [can be] seized and stored while police obtain[] a search warrant to examine their contents, a significant risk exists that evidence contained on a cell phone could be destroyed *by an arrestee's confederates* before the police have the opportunity to obtain a warrant." Pet. for Cert. at 15, *United States v. Wurie*, No. 13-212 (emphasis added). More specifically, the government suggests that during the time necessary to obtain a warrant, third parties might be able to "wipe" – that is, erase – files on an arrestee's smart phone from another computer at a

remote location. *Id.* at 15-16; *see also United States v. Flores-Lopez*, 670 F.3d 803, 807-09 (7th Cir. 2012) (conveying same concern).

No such risk, however, could possibly have existed with respect to the smart phone at issue here. Petitioner's phone stored most of its data – including all photos and videos – on a removable "microSD Card." *Samsung Instinct Touchscreen Cell Phone*, Samsung, http://www.samsung.com/us/mobile/cell-phones/SPH-M800ZKASPR-specs. In fact, the user of this type of phone "*must* have a microSD memory card installed to use the Camera." Samsung Instinct User Guide 108 (2008), *available at* http://support.sprint.com/global/pdf/user_guides/samsung/instinct/samsung_instinct_ug.pdf (emphasis added). Just like similar cards commonly used in digital cameras, anyone, including a police officer, can easily eject a microSD card. And once that is done, the digital data it contains is impervious to third-party tampering.

Even apart from the specifics of petitioner's smart phone, two readily available safeguards enable the police to eliminate the risk posed by remote-wiping technology with respect to *any* cell phone. First, as several courts have recognized, preventing the phone from receiving a signal eliminates the danger of remote wiping. *See, e.g.*, *United States v. Wurie*, 728 F.3d 1, 11 (1st Cir. 2013); *Flores-Lopez*, 670 F.3d at 809. This can usually be accomplished simply by turning (or leaving) the phone off, or putting it into "airplane mode."

If officers are worried for some reason that neither of those options would be a foolproof way of preventing the phone from receiving a signal, all the

officers need to do is place the phone into a lightweight and inexpensive pouch known as a Faraday bag. *Wurie*, 728 F.3d at 11; *see also* Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 Wm. & Mary Bill Rts. J. 601, 607 (2013) (describing Faraday bags); Amicus Br. of Elec. Privacy Info. Ctr. (same). A Faraday bag looks much like a Ziploc freezer bag (usually including a clear window), and prevents radio waves from connecting with the phone inside.

In fact, police departments across the country already use Faraday bags for just this signal-blocking purpose. For several years, the Department of Justice's Cybercrime Lab recommended that police be equipped with Faraday bags and use them whenever necessary to protect against remote wiping of Apple iPhones.[8] The California Department of Justice's Bureau of Forensic Services likewise advises officers to use Faraday bags in order to "[b]lock wireless signals" from reaching mobile devices.[9] Similar evidence of the ease and effectiveness of using Faraday bags abounds. *See* Amicus Br. of Criminal Law Profs. Consequently, if officers are truly

---

[8] *See* Dep't of Justice Computer Crime and Intellectual Prop. Section, Cybercrime Lab, Awareness Brief: Find My iPhone 3 (2009), *available at* http://cryptome.org/isp-spy/iphone-spy.pdf.

[9] Cal. Dep't of Justice, Bureau of Forensic Servs., Physical Evidence Bulletin: Digital Evidence Collection – Mobile Devices 3 (2011), *available at* http://oag.ca.gov/sites/all/files/pdfs/cci/reference/ peb_18.pdf.

concerned about the possibility of an arrestee's confederates attempting to remotely wipe a phone (a concern belied by the officers' actions here), their own training and internal procedures already tell them what to do. And once they follow that guidance, there can be no argument that searching the phone without a warrant is necessary to avoid any potential destruction of evidence.

Second, police can copy, without viewing, the contents of a smart phone so as to create a digital backup. *See Wurie*, 728 F.3d at 11. For example, a Universal Forensic Extraction Device (UFED) can "download all the photos and videos from an iPhone within ninety seconds." Gershowitz, *supra*, at 606; *see also* Christa Miller et al., *What's in an App? Extracting and Examining Mobile Device App Data*, Evidence Tech. Mag., Nov.-Dec. 2013, at 6-9 (extraction "accesses all data on the device, regardless of where it is or was stored"), *available at* http://www.nxtbook.com/nxtbooks/evidencetechnology/20131112/index.php?startid=6#/8. The police, in fact, apparently "downloaded" the data from petitioner's phone in just this manner. J.A. 14. Thus, there can be no claim that the officers lacked the opportunity to preserve all of the phone's digital contents while seeking a warrant advising which data, if any, could be inspected and which had to be left unexamined (and perhaps destroyed).

B. The Degree Of Intrusiveness Of The Search Of Petitioner's Phone Rendered The Search Unreasonable.

"As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a government search is 'reasonableness.'" *Maryland v.*

King, 133 S. Ct. 1958, 1969 (2013) (quoting *Acton*, 515 U.S. at 652). Therefore, even if searching the digital contents of a smart phone without a warrant served some legitimate law enforcement interest, the search in any given case "must [still] be tested by the Fourth Amendment's general proscription against unreasonable searches and seizures." *Edwards*, 415 U.S. at 808 n.9 (alteration in original) (quoting *Terry v. Ohio*, 392 U.S. 1, 20 (1968)); *see also* Pet. for Rehearing En Banc at 6-7, *United States v. Wurie*, 724 F.3d 255 (1st Cir. 2013) ("In cases involving more intrusive searches of computer-like phones, the core Fourth Amendment requirement of reasonableness protects against unwarranted invasions of privacy."). This reasonableness test "requires a court to weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'" *King*, 133 S. Ct. at 1970 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

Conducting an exploratory search of a smart phone's text, photographic, and video files intrudes upon personal privacy to an unprecedented degree. This is so because (1) the text, photo, and video files of modern smart phones – not to mention such phones' vast array of other files – hold exponentially greater amounts and types of sensitive personal information than any physical item an arrestee could carry on his person; and (2) much of that information, unlike typical physical items, implicates First Amendment concerns, such as free expression, private communication, and associational interests.

1. Smart Phones Hold Extraordinary Amounts Of Sensitive Personal Information.

Whether viewed in terms of the Fourth Amendment's historical purpose or modern realities, conducting an exploratory search of the digital contents of a smart phone severely impinges on personal privacy because of the massive amounts of sensitive information such devices contain.

a. The Fourth Amendment's prohibition against unreasonable searches was devised largely as a response to the infamous "general warrants" and "writs of assistance" used in England and America during colonial times. General warrants allowed British officers indiscriminately to "search[] private houses for the discovery and seizure of books and papers," as well as any other evidence, that might be used to convict their owners of crimes. *Boyd v. United States*, 116 U.S. 616, 626 (1886). Writs of assistance similarly permitted "customs officers in the early colonies . . . to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought." *Wurie*, 728 F.3d at 9. The Framers "despised" such searches, *King*, 133 S. Ct. at 1980-81 (Scalia, J., dissenting), "since they placed 'the liberty of every man in the hands of every petty officer,'" *Boyd*, 116 U.S. at 625; *see generally* Amicus Br. of Const. Accountability Ctr. (elaborating on this history).

Just like general warrants and writs of assistance, the California Supreme Court's categorical rule would give law enforcement access to "virtual warehouse[s]" of people's "most intimate communications and photographs" whenever

someone is subject to a custodial arrest. Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L. Rev. 183, 211 (2010). The smart phone in this case, for example, could store up to eight gigabytes of information. Samsung Instinct User Guide, *supra*, at 96. "Apple's iPhone 5 comes with up to sixty-four gigabytes of storage, which is enough to hold about four million pages of Microsoft Word documents." *Wurie*, 728 F.3d at 8 (internal quotation marks and citations omitted).

Given the volume and sensitivity of information on an average person's smart phone, it would be hard to overstate the seriousness of the warrantless intrusions the California Supreme Court's rule would countenance. In text, photo, and video files alone, a typical phone contains private notes, back-and-forth conversations, and snapshots spanning several years – an array of information formerly impossible for an officer to obtain incident to an arrest. Indeed, insofar as such files reflect one's daily thoughts, wonders, and concerns, they are in many ways "an extension of [one's] mind." Stephen Shankland, *How Google Is Becoming an Extension of Your Mind*, CNET (July 16, 2012), http://news.cnet.com/8301-1023_3-57470853-93/how-google-is-becoming-an-extension-of-your-mind/. And this is to say nothing of other information – from personal calendars to banking and health records, to privileged and confidential business emails and memoranda, to historic GPS location information – that is increasingly intertwined with text and photo files by means of "alert" and "notification" protocols, as well as other data integration systems.

A modern smart phone, in short, is a compact, yet powerful, computer that happens to include a phone.[10] It is a portal into our most sensitive and confidential affairs. The digital contents of such a device should not be subject to a fishing expedition for evidence of whatever suspicious thoughts or activities an officer might discover.

b. This is not to deny that arrests have consequences, including subjecting arrestees to "reduced expectations of privacy caused by the arrest." *Diaz*, Pet. App. 35a-36a (quoting *Chadwick*, 433 U.S. at 16 n.10); *see also King*, 133 S. Ct. at 1978. But having one's expectation of privacy diminished "to a reasonable extent," *Edwards*, 415 U.S. at 809 (internal quotation marks and citation omitted), is not the same as having it completely wiped out. Therefore, while being arrested shrinks a person's privacy in, say, his clothing, *see id.*, it does not deprive him of the Fourth Amendment's core protection against general searches through his most sensitive information. And that core protection forbids the government from "rummaging through [an arrestee's] electronic private effects – a cell phone – without a warrant." *State v. Granville*, ___ S.W.3d ___, 2014 WL 714730, at *1 (Tex. Crim. App. Feb. 26, 2014). As the Texas Court of Criminal Appeals recently put it, searching a person's smart phone "is

---

[10] Indeed, "the government admitted at oral argument [in the First Circuit in *Wurie*] that its interpretation of the search-incident-to-arrest exception would give law enforcement broad latitude to search *any* electronic device seized from a person during his lawful arrest, including a laptop computer or a tablet device such as an iPad." *Wurie*, 728 F.3d at 7 (emphasis added).

not like [searching] a pair of pants or a shoe"; it is "like searching his home desk, computer, bank vault, and medicine cabinet all at once." *Id.* at *6-7. Such is the essence of a general search.

Indeed, even before the advent of digital storage devices, this Court observed in *Chimel* that "[a]fter arresting a man in his house, to rummage at will among his papers in search of whatever will convict him, appears to us to be indistinguishable from what might be done under a general warrant." 395 U.S. at 767 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.)). More recently in *Gant*, this Court likewise barred exploratory searches of automobiles incident to arrest in part because "the character of that threat implicates the central concern underlying the Fourth Amendment – the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." 556 U.S. at 345 & n.5 (internal quotation marks and citation omitted).

The same reasoning applies – only more so – to rummaging at will through a smart phone that a person is carrying when arrested. Before the development of smart phones, people kept the information stored on such devices only in the most private recesses of their homes or offices, safely beyond the reach of any search that might occur incident to arrest. The protection the Fourth Amendment has always afforded to such information should not evaporate – more than two hundred years after the Founding – simply because that information can now be reduced to electronic charges in a computer chip and carried in one's pocket.

c. Practical considerations relating to the Fourth Amendment's default warrant requirement reinforce the intrusiveness of exploratory searches of smart phones incident to arrest. "A warrant serves primarily to advise the citizen that an intrusion is authorized by law and limited in its permissible scope and to interpose a neutral magistrate between the citizen and the law enforcement officer 'engaged in the often competitive enterprise of ferreting out crime.'" *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 667 (1989) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)); *see also United States v. Lefkowitz*, 285 U.S. 452, 464 (1932) ("Security against unlawful searches is more likely to be attained by resort to search warrants than by reliance upon the caution and sagacity of petty officers while acting under the excitement that attends the [arrest] of persons accused of crime."). Consequently, the need for a warrant is greatest when an officer has vast discretion that a magistrate can limit by specifying with particularity what the officer may and may not inspect. On the other hand, "[t]he need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the 'interpo[lation] of a neutral magistrate between the citizen and the law enforcement officer.'" *King*, 133 S. Ct. at 1969-70 (alteration in original) (quoting *Von Raab*, 489 U.S. at 667).

Conducting the kind of search of a smart phone that the police conducted here obviously falls into the former category. The record does not disclose how many digital files and applications the officers searched. But we know that officers "had no idea" what they might find and looked through "a lot of stuff" – including, at a minimum, the phone's text

entries, phone numbers, and the photo and video files. BIO 12; J.A. 8, 11, 14, 20. That is more than enough to show that the officers conducted an unbounded, exploratory search of petitioner's phone for any evidence they might find to convict him of a crime.

In light of the innumerable digital files and applications that modern smart phones contain, it simply will not work to leave it to police officers to exercise discretion over which files to search, how far back in time to search, and which attachments or links to activate. Only by requiring warrants "particularly describing the place[s] to be searched," U.S. Const. amend. IV, can courts ensure that any investigative search of a smart phone "will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

2. Smart Phones Hold Information That Implicates First Amendment Concerns.

Searching the digital contents of a smart phone incident to arrest for evidence of criminality is unreasonable for another reason: it implicates constitutional interests in safeguarding private communications, as well as free expression and association, from official intrusion.

1. The Framers believed that, "[o]f all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than . . . exemption of his private affairs, books, and papers from the inspection and scrutiny of others."

Interstate Commerce Comm'n v. Brimson, 154 U.S. 447, 479 (1894) (internal quotation marks and citation omitted). That was not merely a theoretical belief; it was based on bitter experience. "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961).

In particular, "those who framed the Fourth Amendment" were keenly familiar with the infamous English cases of *Wilkes v. Wood*, (1763) 98 Eng. Rep. 489 (C.P.), 19 How. St. Tr. 1153, and *Entick v. Carrington*, (1765) 95 Eng. Rep. 807 (C.P), 19 How. St. Tr. 1029. *See Boyd*, 116 U.S. at 625-27. In both cases, officers arrested publishers of opposition newspapers in their homes for seditious libel and searched and seized their private papers. *See Boyd*, 116 U.S. at 625-26 (describing *Wilkes* case); *Entick*, 95 Eng. Rep. at 807, 19 How. St. Tr. at 1030 (noting that officers "broke open, and read over, pryed into, and examined all of the private papers" in the home over a four-hour period). Emphasizing the special sanctity of private papers, Lord Camden declared the searches "totally subversive of the liberty of the subject[s]," *Wilkes*, 98 Eng. Rep. at 498, 19 How. St. Tr. at 1167, and "subversive of all the comforts of society," *Entick*, 95 Eng. Rep. at 817-18, 19 How. St. Tr. at 1066. "[E]very American statesmen" agreed with these assessments and "considered [them] as the true and ultimate expression of constitutional law" in the country's new charter. *Boyd*, 116 U.S. at 626; *see also Stanford v. Texas*, 379 U.S. 476, 484 (1965) (describing *Entick* as the "wellspring of the rights now protected by the Fourth Amendment").

In light of this history, this Court has held that the Fourth Amendment imposes "special constraints upon searches for and seizures of material arguably protected by the First Amendment." *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 n.5 (1979). In *Marcus*, 367 U.S. at 730-38, and *Stanford*, 379 U.S. at 485, for instance, this Court held that warrants allowing the search and seizure of expressive materials must specify with heightened particularity exactly what may be inspected. As the Court later explained in a case dealing with a police search of photographs: "Where presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field." *Zurcher v. Stanford Daily*, 436 U.S. 547, 551-52, 564 (1978). Furthermore, when seizure of materials covered by the First Amendment may prevent the dissemination of speech or other expression, a special predeprivation hearing is necessary. *See A Quantity of Copies of Books v. Kansas*, 378 U.S. 205, 210-11 (1964). Finally, "[t]his Court has recognized the vital relationship between freedom to associate and privacy in one's associations," holding that people's relationships to groups involved in "political, economic, religious, or cultural matters" are entitled to remain confidential absent an especially strong governmental need for disclosure. *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460-62 (1958); *see also Jones*, 132 S. Ct. at 956 (Sotomayor J., concurring) ("Awareness that the

government may be watching chills associational and expressive freedoms.").[11]

The search-incident-to-arrest doctrine has had a "checkered history." *Gant*, 556 U.S. at 350. But this Court has consistently indicated that the doctrine – like the other Fourth Amendment doctrines just discussed – contains special limitations on searching expressive or associational materials. Most notably, in *Lefkowitz*, 285 U.S. at 467, this Court held that officers violated the Fourth Amendment by conducting an exploratory search of a person's books and papers in his office incident to arrest. Relying on Lord Camden's declaration in *Entick* that "one's papers are his dearest property," this Court reasoned that police officers may not search a person's private

---

[11] To the extent the cases in the preceding paragraph allow the search and seizure of private communications and other expressive documents pursuant to properly drawn warrants and other procedural protections, this jurisprudence diverges from the even stricter, original understanding of the Fourth Amendment. As originally conceived, reaffirmed in *Boyd*, and generally enforced until the 1960s, the Fourth Amendment flatly forbade the search or seizure of any private papers – regardless of any warrant or other judicial or legislative sanction – for purposes of gathering evidence to use against someone in a criminal prosecution. *See Boyd*, 116 U.S. at 622-24, 630; *see generally* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 50 (2013); Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869, 869-70 (1985). Hence, to the extent this case turns solely on what "the Framers of the Fourth Amendment would have considered 'reasonable,'" *City of Indianapolis v. Edmond*, 531 U.S. 32, 56 (2000) (Thomas, J., dissenting), it is a straightforward case and reversal is required.

papers incident to arrest to find evidence of the crime of arrest or some other crime. *Lefkowitz*, 285 U.S. at 464-66.

Other decisions over the years have implicitly recognized the unreasonableness of searching personal communications incident to arrest. In *Harris v. United States*, 331 U.S. 145, 154 (1947), this Court held that the Fourth Amendment permitted police officers to inspect and seize an envelope containing draft cards from a drawer in an arrestee's apartment. This Court, however, emphasized that "[c]ertainly this is not a case of search for or seizure of an individual's private papers." *Id.* at 154 & n.18. When this Court later overruled *Harris*, it cited with approval Judge Learned Hand's opinion for the Second Circuit in *Kirschenblatt*, 16 F.2d at 203. *See Chimel*, 395 U.S. at 767-68. Judge Hand explained in that opinion that "the whole of a man's correspondence, his books of account, the record of his business, in general, the sum of his documentary property . . . are as inviolate upon his arrest as they certainly are upon search warrant." *Kirschenblatt*, 16 F.2d at 204; *see also* Taylor, *supra*, at 70 ("There is no good reason why a diary or personal letter, otherwise immune, should be subject to seizure when found on the arrestee's person.").

The problem with exploratory searches through even tangible private papers is that they invariably expose protected expression and communications to governmental scrutiny. As Judge Friendly put it years ago, "The reason why we shrink from allowing a personal diary to be the object of a search is that the entire diary must be read to discover whether

there are incriminating entries." *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969). The same problem inheres in "'rummaging' through the contents of a desk to find an incriminating letter." *Id.*; *see also* Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869, 918 (1985) ("Because papers cannot be so easily distinguished from each other, a typical search is necessarily a rummaging search of the most intrusive kind."). Private papers, in short, reside at the apex of our privacy hierarchy, so it is unreasonable for police officers to examine such documents in conjunction with an arrest beyond the degree to which necessary to ensure that they do not hold any weapons or other threatening physical items.

2. For the same reasons, it is unreasonable for the police to conduct an exploratory search of the digital contents of a smart phone seized incident to arrest. *See* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 109 (2013). Conducting such a search is the modern counterpart to examining "the whole of a man's correspondence, his books of account, the record of his business, in general, the sum of his documentary property." *Kirschenblatt*, 16 F.2d at 204. Even when the police limit their search (as they may have done here) to a phone's photo, video, and certain text files, the intrusion is still dramatic and wide-ranging. Such files hold personal, often intimate, material that people may not have even ventured to capture in

visible form before the advent of smart phones.[12] Indeed, as this Court observed a few Terms ago, "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010).

Searching through photographs, videos, contacts lists, text messages, and other material in smart phones also presents insoluble associational risks. Photographic material, by its very nature, tends to reveal one's personal and professional relationships. Contacts lists and email groups show one's web of connections even more holistically. Text messages can be similarly revealing. Finally, the very existence of certain applications on a smart phone – imagine, for instance, an icon on a phone's home screen for the Libertarian Party, the Nation of Islam, or Greenpeace – can disclose one's most sensitive memberships and beliefs.

The search of petitioner's smart phone implicated nearly all of these concerns. The police searched the digital contents of petitioner's smart phone because

---

[12] It bears remembering that when the police are allowed to rummage through such material, the risk is not only that they will see potentially embarrassing, politically sensitive, or confidential business documents. They may also disseminate or otherwise misuse the information they discover. *See, e.g.*, *Newhard v. Borders*, 649 F. Supp. 2d 440, 443-44 (W.D. Va. 2009) (noting that after the police arrested a school teacher for a DUI, they searched his cell phone and found sexually explicit photos of him and his girlfriend and then shared the photos with other officers and members of the public).

they wanted to look around for evidence of criminality. J.A. 23. What is more, there was nothing targeted about the search. Detective Malinowski rifled through pictures, watched videos to see what might "ca[tch] [his] eye," and scanned phone numbers in order to discover – among other things – petitioner's connections. *Id.* 8, 30. Such exploratory searches of expressive and associational material strike at the heart of the Fourth Amendment and cannot be countenanced.

C. Limiting Searches Of Smart Phones To Situations In Which Officers Believe Such Phones Contain Evidence Of The Crime Of Arrest Would Not Solve The Constitutional Problems Inherent In Such Searches.

Although the California Court of Appeal and trial court rested their rulings here exclusively on the California Supreme Court's categorical ruling that police may always rummage through any smart phone seized from an arrestee, *see* Pet. App. 15a; J.A. 26, the trial court observed at one point that the gang detective who conducted the exploratory search of petitioner's phone "testified that in his experience persons and gang members do take photos of themselves and their crimes and he expected there could be such photos on the cell phone." J.A. 23. Nothing about this testimony, however, legitimized the search in this case. This Court held in *Gant* that "when it is reasonable to believe evidence relevant to the crime of arrest might be found in [a] vehicle," police may lawfully search the automobile incident to arrest. 556 U.S. at 343 (internal quotation marks and citation omitted). But, contrary to the federal

government's argument, *see* Pet. for Cert. 18, *United States v. Wurie*, No. 13-212, that holding does not apply to cell phones – and even if it did, the reasonable belief standard would not be satisfied here.

1. *Gant*'s reasonable belief rule derives from "circumstances *unique* to the vehicle context." 556 U.S. at 343 (emphasis added). Three such circumstances bear emphasis here. First this Court has long recognized that, because of their inherent mobility, automobiles "can be quickly moved out of the locality or jurisdiction in which the warrant must be sought." *Carroll v. United States*, 267 U.S. 132, 153 (1925). Even when placed in impound lots, vehicles are "susceptible to theft or intrusion by vandals." *Chadwick*, 433 U.S. at 13 n.7. Second, "[t]he search of an automobile is far less intrusive on the rights protected by the Fourth Amendment than the search of one's person or of a building" because an automobile "seldom serves as one's residence or as the repository of personal effects." *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (internal quotation marks and citation omitted). Third, individuals have a reduced expectation of privacy in an automobile "owing to its pervasive regulation." *Pennsylvania v. Labron*, 518 U.S. 938, 940 (1996) (per curiam) (citing *California v. Carney*, 471 U.S. 386, 391-92 (1985)). After all, automobiles "are subjected to police stop and examination to enforce 'pervasive' governmental controls '[a]s an everyday occurrence.'" *Wyoming v. Houghton*, 526 U.S. 295, 303 (1999) (alteration in original) (quoting *South Dakota v. Opperman*, 428 U.S. 364, 368 (1976)).

Not one of these circumstances is present when the police have seized a smart phone from an arrestee. First, once reduced to police control, a smart phone cannot disappear and is easily secured against theft or vandalism. Second, a modern cell phone's primary use is as a repository of private papers and information – "the kind of information one would have previously stored in one's home," *Wurie*, 728 F.3d at 8, not in one's car. Put another way, most people regularly allow others to see the interior and contents of their cars, *see Cardwell*, 417 U.S. at 590-91, but not their phones. Third, police officers do not regularly review the content of text, photo, or video files on smart phones for any regulatory or administrative purpose.

In sum, automobiles hold a singular place in Fourth Amendment law. There is no good reason to extend *Gant*'s reasonable belief exception beyond that context – let alone to a context as dramatically different as smart phones.

2. What is more, applying *Gant*'s reasonable belief exception to smart phones would swallow any general rule banning such warrantless searches incident to arrest. In *Gant*, this Court perceived the reasonable belief exception as a genuine exception to the warrant requirement, noting that "[i]n many cases . . . there will be no reasonable basis to believe the vehicle contains relevant evidence." 556 U.S. at 343. By contrast, precisely because of the wealth of information contained on smart phones, it is difficult to imagine a crime of arrest where police could not at least claim to believe a phone would contain relevant evidence.

Consider the files we know the police examined in this case. People now take photos and videos of themselves (sometimes called "selfies") and their activities on a daily, if not hourly, basis.[13] People create and receive text entries even more often. Insofar as such pictures and words continually document one's daily doings and whereabouts, they are inherently likely to interest officers investigating potential criminal behavior. Similarly, phone numbers stored in one's contacts folder and call logs list one's acquaintances and catalogue one's interactions with them. An arresting officer, therefore, might think that such folders and logs are inherently subject to warrantless inspection because they identify potential witnesses for investigating and prosecuting the crime of arrest.

The phone seized from petitioner – like all smart phones – also contained other tools and sensors that collect and store data on users. For example, petitioner's smart phone collected and stored GPS location data. Samsung Instinct User Guide, *supra*, at 200. Such data generates a historical record of the owner's movements, *see Jones*, 132 S. Ct. at 963 (Alito, J., concurring in judgment), such that it might reveal the speed at which his car was traveling before being pulled over or whether he stopped on the way home from work to have a couple drinks. Internet

---

[13] *See* Molly Wood, *Narcissist's Dream: Selfie-Friendly Phone*, N.Y. Times, Feb. 6, 2014, at B1; *Digital Photos Taken by Americans*, Nat'l Geographic, April 2012, at 35.

browsers store users' search histories and product purchases. The list goes on and on.[14]

The point is that when almost all aspects of a person's life are channeled through a single device, a curious police officer will virtually always be able to assure himself that he has reason to believe that an arrestee's smart phone contains evidence of the crime(s) of arrest. And if all it takes for an officer to conduct a warrantless, exploratory search is such an assurance with respect to *something* that might be *somewhere* on the phone, then the federal government's *Gant*-based argument is really no different from the California Supreme Court's position that officers should always be able to search smart phones seized from arrestees.

If anything, a *Gant*-based regime would be worse. By holding out a promise restricting law enforcement authority to search smart phones, a *Gant*-based regime would encourage defendants always to challenge whether (or to what extent) the reasonable-belief standard was satisfied in their cases. Yet because those legal limits would be largely illusory, almost all of this litigation would ultimately be for naught.

---

[14] In addition to GPS data, more recent smart phones include other sensors such as a compass, accelerometer, gyroscope, fingerprint reader, proximity sensor, barometer, thermometer, and humidity sensor. *See, e.g.*, *Apple – iPhone 5s – Technical Specifications*, Apple, http://www.apple.com/iphone-5s/specs/; *Samsung Galaxy S4 – Life Companion*, Samsung, http://www.samsung.com/ global/microsite/galaxys4/.

3. The facts of this case reinforce how inappropriate it would be to apply *Gant*'s reasonable belief rule to the context of smart phones. Petitioner was arrested for concealing a firearm within a vehicle and carrying a loaded weapon. *See* Cal. Penal Code § 12025(a)(1) (current version at § 25400(a)(1)); Cal. Penal Code § 12031(a)(1) (current version at § 25850(a)(1)). As summarized by the trial court, the officer who searched petitioner's phone "testified that in his experience persons and gang members do take photos of themselves and their crimes and he expected there could be such photos on the cell phone." J.A. 23.

Petitioner believes that this assertion falls short of constituting a "reasonable belief" that evidence of petitioner's crime of arrest would be found on his smart phone. After all, the officer's testimony really amounts to nothing more than an assertion that people often take pictures of themselves doing the things they do. But if the State argues the *Gant* standard is satisfied here, that argument would simply illustrate how ill-suited to the digital contents of smart phones any reasonable belief test would be. Surely the proposition that human beings often take photos of themselves – or its equivalent with respect to text entries, GPS data, or other information stored on smart phones – should not be enough to justify dispensing with a default warrant requirement.

II. The Search Of Petitioner's Phone At The Stationhouse Was Too Remote From His Arrest To Qualify As A Search Incident To Arrest.

The search of petitioner's smart phone at the stationhouse, during which the officers found the videos and photographs that the prosecution later introduced into evidence, violated the Fourth Amendment for another reason: a search of an item two hours after an arrest at a police station is not truly "incident" to arrest. In fact, numerous lower courts already have held as much in cases indistinguishable from this one.[15]

1. This Court has repeatedly emphasized that "a search 'can be incident to an arrest only if it is substantially contemporaneous with the arrest and is confined to the *immediate* vicinity of the arrest.'" *Shipley v. California*, 395 U.S. 818, 819-20, (1969) (per curiam) (quoting *Stoner v. California*, 376 U.S. 483, 486 (1964)); *accord New York v. Belton*, 453 U.S. 454, 457, 462 (1980); *Roaden v. Kentucky*, 413 U.S. 496, 497 (1973); *Preston v. United States*, 376 U.S.

---

[15] *See United States v. Gibson*, No. CR 11-00734 WHA, 2012 WL 1123146, at *9-10 (N.D. Cal. 2012) (search of phone "one or two hours after arresting defendant" was too remote from arrest to be "incident" to it); *United States v. DiMarco*, No. 12 CR 205(RPP), 2013 WL 444764, at *10-12 (S.D.N.Y. 2013) (six-hour delay; same result); *United States v. Yockey*, No. CR09-4023-MWB, 2009 WL 2400973, at *5 (N.D. Iowa 2009) (search after defendant was booked in jail; same result), *report and recommendation adopted*, 654 F. Supp. 2d 945; *State v. Isaac*, 209 P.3d 765, No. 101,230, 2009 WL 1858754, at *5 (Kan. Ct. App. 2009) (search "more than an hour after Isaac's arrest while Isaac was being booked into jail"; same result).

364, 367 (1964); *Agnello v. United States*, 269 U.S. 20, 30-31 (1925). If the search is "remote in time or place from the arrest," the search-incident-to-arrest-doctrine no longer justifies it. *Preston*, 376 U.S. at 367.

The reason for these limitations is simple: the search-incident-to-arrest doctrine is designed to protect law enforcement's interests in disarming arrestees and preventing them from destroying evidence. Once the police accomplish these tasks by seizing any items of interest at the scene and retreating to the safety of the police station, neither of those interests retains any force – and a warrantless search, therefore, becomes unreasonable absent some other justification. *See Preston*, 376 U.S. at 367; *see also Bailey v. United States*, 133 S. Ct. 1031, 1042-43 (2013) (once justifications for an exception to the warrant requirement vanish, so does police authority to conduct a warrantless search); *Arizona v. Gant*, 556 U.S. 332, 338-39 (2009) (same).

Two decisions from this Court illustrate this point and, for all practical purposes, dictate the outcome here. First, in *Preston*, officers arrested a man who was standing next to his car. 376 U.S. at 365. The Court "assume[d]" that "the police had the right to search the car when they first came on the scene." *Id.* at 367-68. But instead of doing so, the police simply seized the car and took it (along with the defendant) to the police station. *Id.* at 365. Soon after the defendant was booked, the officers conducted a general search of the car and discovered evidence of additional crimes. *Id.*

This Court held unanimously that "the search was too remote in time or place to have been made as

incidental to the arrest and . . . therefore, that the search of the car without a warrant failed to meet the test of reasonableness under the Fourth Amendment." *Preston*, 376 U.S. at 368. As this Court succinctly explained, "[o]nce an accused is under arrest and in custody, then a search made at another place, without a warrant, is simply not incident to the arrest." *Id.* at 367. This is especially so when the accused is safely detained at the station house and the police have exclusive control over the items they wish to search. Under those circumstances, this Court stressed, there can be no argument that the accused might gain access to the property and obtain a weapon or "destroy[] any evidence of a crime." *Id.* at 368.

Four years later, this Court reiterated this limitation on the search-incident-to-arrest doctrine in *Dyke v. Taylor Implement Mfg. Co.*, 391 U.S. 216 (1968). There, as in *Preston*, the police arrested a person for a traffic offense and took him and his car to the county jail. *Id.* at 218-19. With the arrestee in custody inside, officers searched the vehicle. *Id.* at 219. This Court again held with little difficulty that the search violated the Fourth Amendment. *Id.* at 220. Drawing on *Preston*, this Court reasoned that "under such circumstances, a search is 'too remote in time or place to [be] incidental to the arrest.'" *Id.* (quoting *Preston*, 376 U.S. at 368).

This Court later limited the reach of *Preston* and *Dyke* with respect to vehicles, holding that the "automobile exception" allows officers to conduct delayed searches of cars seized at the time of arrest, when there is probable cause to believe the cars contain evidence of illegality. *See Chambers v.*

Maroney, 399 U.S. 42, 52 (1970). But the remoteness principle otherwise has retained its vitality. In *United States v. Chadwick*, 433 U.S. 1 (1977), for instance, this Court explained that "warrantless searches of luggage or other property seized at the time of an arrest cannot be justified as incident to that arrest either if the 'search is remote in time or place from the arrest.'" *Id.* at 15 (quoting *Preston*, 376 U.S. at 367). Accordingly, this Court held that the search of an arrestee's footlocker at the stationhouse "more than an hour after [the] agents had gained exclusive control" over it could not "be viewed as incidental to the arrest." *Id.*; *see also Cardwell v. Lewis*, 417 U.S. 583, 591 n.7 (1974) (holding that a "difference in time and place eliminates any search-incident-to-an-arrest contention"). Similar lower court decisions abound.[16]

---

[16] In one leading case, the D.C. Circuit (per Judges Randolph, Mikva, and Silberman), held that a search of an arrestee's suitcase between thirty and sixty minutes after arrest was too remote to be incident to arrest. *United States v. $639,558 in U.S. Currency*, 955 F.2d 712, 716-17 & n.7 (D.C. Cir. 1992). For equivalent decisions, see *United States v. Butler*, 904 F.2d 1482, 1484-85 (10th Cir. 1990) (jewelry box); *United States v. Vasey*, 834 F.2d 782, 787-88 (9th Cir. 1987) (luggage); *United States v. Montalvo-Cruz*, 662 F.2d 1285, 1290 (9th Cir. 1981) (purse); *United States v. Schleis*, 582 F.2d 1166, 1172 (8th Cir. 1978) (locked briefcase), *abrogated on other grounds by United States v. Morales*, 923 F.2d 621 (8th Cir. 1991); *Commonwealth v. Pierre*, 893 N.E.2d 378, 384 (Mass. App. Ct. 2008) (plastic bags that arrestee was carrying); *State v. Murray*, 605 A.2d 676, 680 (N.H. 1992) (purse); *People v. Redmond*, 390 N.E.2d 1364, 1374 (Ill. App. Ct. 1979) (purse).

The search-incident-to-arrest doctrine's remoteness limitation applies with full force to the police's search of the photo and digital files of petitioner's smart phone. When Officer Malinowski commenced that search, petitioner had been under arrest for "about two hours." BIO 2. He had been booked and was securely in police custody. And the officers had petitioner's smart phone exclusively in their possession at the station house with no chance whatsoever that petitioner could gain access to it. If the police were concerned that any digital evidence contained in the phone might evaporate, all the officers had to do was simply freeze the phone's contents by placing it in a Faraday bag or similar device, or download them to a secure place pending a request for a search warrant. *See supra* at 22-24. Because the police took neither of these steps, the station house search of the phone was unreasonable.

2. The California Supreme Court has resisted this analysis, contending that this Court's decision in *United States v. Edwards*, 415 U.S. 800 (1974), permits "delayed" searches of items seized incident to arrest whenever those items were taken from the person of (in contrast to the immediate vicinity of) the arrestee. *Diaz*, Pet. App. 33a & n.5. The California Court of Appeal thus held in this case that the remoteness in time and space of the officers' search of petitioner's smart phone was irrelevant. Pet. App. 15a.

This reasoning overreads *Edwards*. In that case, the police arrested the defendant for attempted breaking and entering and placed him in jail. 415 U.S. at 801. Several hours later, the police learned that the shirt he was still "wearing at the time of and

since his arrest," might contain paint chips constituting useful evidence against him. *Id.* at 802. The police thus directed him to remove the shirt and examined it for paint chips. *Id.* This Court held that the seizure and examination of the shirt were reasonable. *Id.* at 803. Quoting this Court's earlier decision in *Abel v. United States*, 362 U.S. 217 (1960), this Court explained that "when the accused decides to take the property with him" after being arrested, it does not contravene the Fourth Amendment for the police to seize and search the property "at the first place of detention." *Edwards*, 415 U.S. at 803 (quoting *Abel*, 362 U.S. at 239) (internal quotation marks omitted).

The *Edwards* rule permitting officers to seize and inspect items on an arrestee's person at the police station thus turns not on whether the property was immediately associated with the arrestee's person *at the time of arrest*, but rather on the more specific inquiry whether the property was *still "in his possession at the place of detention."* *Id.* at 807 (emphasis added). This makes perfect sense. When "the accused decides to take property with him" to the police station, *id.*, then it is possible right up until the time of the search that he might use the property as a weapon or as a tool for attempting an escape. By contrast, when the police seize property at the scene, neither possibility exists later at the police station while the property is "under the exclusive dominion of police authority," *Chadwick*, 433 U.S. at 15, and the arrestee is in a jail cell.

To be sure, there is a sentence in *Edwards* suggesting that the Fourth Amendment permits searches of clothing or effects immediately associated

with an arrestee's person to be conducted even "at a later time" than the initial seizure. 415 U.S. at 807. This does not seem to describe what occurred in *Edwards*; as far as can be gleaned from this Court's opinion, the police there seized the arrestee's clothing and then examined it right away for the presence of paint chips.[17] At any rate, *Edwards*' tolerance for delayed searches emanates not from search-incident-to-arrest jurisprudence but rather – as *Edwards* itself indicated – from the inventory-search doctrine first enunciated in *Cooper v. California*, 386 U.S. 58 (1967); *see also Edwards*, 415 U.S. at 806 (citing and discussing *Cooper*). Under that doctrine, the police may search an arrestee's items at any point after their seizure in order to "inventory property found on the person" who has been put in jail. *Illinois v. Lafayette*, 462 U.S. 640, 646-47 (1983). That is, the authority that *Edwards* describes to conduct delayed searches flows not from the accused's arrest, but rather from his "administrative processing," *Edwards*, 415 U.S. at 807.

That authority is immaterial here. The trial court expressly found that the search was "investigative," not administrative, in nature. J.A. 23. The State has never challenged that finding. Nor has the State ever suggested that searching the

---

[17] Even if the police conducted a search of the clothing some period of time after seizing it, the defendant never challenged any such search apart from the seizure itself.

digital contents of a smart phone could ever be justified on the basis of an inventory search.[18]

Any rule subjecting property seized at the scene from the arrestee's person – but not property that was then merely in his grab area – to delayed investigative searches would also lead to intolerably arbitrary results. Under such a rule, the police could conduct delayed searches of the digital contents of any cell phone taken from someone's hands or pockets. But if, for example, the police arrested someone in her office at a moment when the arrestee's cell phone was sitting on her desk, then no delayed search would be permissible. Or if police arrested the driver of a car, they might be unable to conduct a delayed search of a phone resting in a cupholder. Exploratory governmental access to the most sensitive details of a person's private life should hinge on more than such happenstance.

3. One final reason – unique to smart phones and other devices with access to cellular signals – exists for strictly enforcing the remoteness limitation on

---

[18] Nor would any such suggestion have any merit. It fully serves the police interest in conducting an inventory of all seized items to create a list of all *physical* items (including any smart phone itself) seized from an arrestee; the police need not read through "materials such as letters or checkbooks that touch upon intimate areas of an individual's personal affairs," much less digital records of such communications and records. *South Dakota v. Opperman*, 428 U.S. 364, 380 & n.7 (1976) (Powell, J., concurring) (internal quotation marks and citation omitted); *see also D'Antorio v. State*, 926 P.2d 1158, 1162-64 (Alaska 1996) (collecting other authorities); *State v. Davis*, 742 P.2d 1356, 1360-61 (Ariz. Ct. App. 1987) (diary).

searches incident to arrest in this context. When the police seize a package containing purely physical contents, the contents of that package will be exactly the same later at the police station as they were when seized in the field at the time of arrest. By contrast, if, after seizing a smart phone, a police officer forgets or decides not to immediately block it from receiving a signal, the digital contents of the phone will likely *not* be the same later at the police station. Here, for example, the police waited some two hours to resume searching petitioner's smart phone, and there is no indication that they ever disconnected the phone from its network. A typical person receives several emails and text messages per hour, not to mention voice mails and alerts from other applications synching with the internet.

Hence, even if the California Supreme Court were correct, as a general matter, that the search-incident-to-arrest doctrine allows police officers to conduct delayed searches of personal items seized at the time of arrest, that rule could not be applied to smart phones. There is no conceivable reason why seizing a device at the time of arrest should allow the police to use that device to gather and review new information that did not even exist when the device was seized. Indeed, using an arrestee's smart phone to retrieve and inspect such new information without a warrant may implicate not only the Fourth Amendment, but also federal wiretapping statutes, *see* 18 U.S.C. §§ 2511-2522 (making it unlawful for governmental entities to intercept wire communications without meeting a series of statutory requirements), and the Stored Communications Act, *see* 18 U.S.C. §§ 2701, 2703(a) (making it unlawful for governmental entities to retrieve electronic

communications, such as email, from service providers without a warrant).

It is unclear in this case whether the police viewed any information on petitioner's smart phone that came into existence after his arrest. Presumably the photos and videos that the prosecution ultimately introduced into evidence were on the phone before petitioner was arrested. But even these types of digital files on certain smart phones can automatically pull down new information from the "cloud" or other computers. *See, e.g., iCloud Photo Sharing*, Apple, https://www.apple.com/icloud/icloud-photo-sharing.html (describing Apple service that synchronizes a photo and video stream across multiple devices and even across multiple users). And it can be extremely difficult to decipher which files on a smart phone are sealed off from the outside world and which – if left connected to a signal – continually accumulate new information from the internet at large. This reality provides all the more reason why it is vital that the Fourth Amendment incentivize police officers to freeze immediately the contents of smart phones seized incident to arrest – and to require them to seek particularized approval from a magistrate before inspecting any digital files.

CONCLUSION

For the foregoing reasons, the judgment of the California Court of Appeal should be reversed.

Respectfully submitted,

Patrick Morgan Ford
LAW OFFICE OF PATRICK
MORGAN FORD
1901 First Avenue
Suite 400
San Diego, CA 92101

Donald B. Ayer
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001

Jeffrey L. Fisher
Counsel of Record
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

March 3, 2014

RESPONDENT'S BRIEF

RECORD
AND
BRIEFS

No. 13-132

Supreme Court, U.S.
FILED
APR - 2 2014
OFFICE OF THE CLERK

In The
Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ Of Certiorari To The California Court Of Appeal, Fourth District

BRIEF FOR RESPONDENT

KAMALA D. HARRIS
Attorney General of California
EDWARD C. DUMONT
Solicitor General
DANE R. GILLETTE
Chief Assistant Attorney General
JULIE L. GARLAND
Senior Assistant Attorney General
STEVEN T. OETTING
CRAIG J. KONNOTH
Deputy Solicitors General
CHRISTINE M. LEVINGSTON BERGMAN*
Deputy Attorney General
STATE OF CALIFORNIA
DEPARTMENT OF JUSTICE
110 West A Street, Suite 1100
San Diego, CA 92101
(619) 645-2247
Christine.Bergman@doj.ca.gov

* *Counsel of Record*

Library of Congress
Law Library

QUESTIONS PRESENTED

Whether evidence admitted at petitioner's trial was obtained in a search of petitioner's cell phone that violated petitioner's Fourth Amendment rights.

TABLE OF CONTENTS

Page

Statement 1

Summary of Argument 7

Argument 10

I. Under existing law, the police were entitled to search photos and videos on petitioner's phone as an incident to his lawful arrest 10

A. The law has long allowed police to search objects found on the person of an individual who is lawfully arrested 11

B. Cases addressing searches of the area of an arrest have not questioned the categorical rule applicable to the arrestee's person and effects 16

C. The evidence at issue here was properly obtained under any standard 22

1. The photos and videos were found in searches of an object recovered from petitioner's person during his arrest 23

2. The searches here were reasonably related to the crime of arrest 28

3. A cell phone such as petitioner's presents safety, identification, and evidentiary issues at least as powerful as those relating to other items routinely seized and searched incident to arrest 29

TABLE OF CONTENTS – Continued

Page

a. Safety and identification 30

b. Preservation of evidence 33

II. The technological advances that petitioner highlights do not warrant the adoption of special rules for cell phones in this case 41

A. The information taken from petitioner's phone is not fundamentally different from that found in other searches incident to arrest 43

B. The circumstances of this case suggest no basis for specially limiting cell phone searches incident to arrests 51

Conclusion 58

TABLE OF AUTHORITIES

Page

CASES

Arizona v. Gant, 556 U.S. 332 (2009).....20, 28

Boyd v. United States, 116 U.S. 616 (1886) 49

California v. Acevedo, 500 U.S. 565 (1991).....18

Catsouras v. Department of the California Highway Patrol, 181 Cal. App. 4th 856 (2010).....54

Chimel v. California, 395 U.S. 752 (1969)....16, 17, 19, 20

Cooper v. California, 386 U.S. 58 (1967) 37

Curd v. City Court of Judsonia, Arkansas, 141 F.3d 839 (8th Cir. 1998) 45

Dillon v. O'Brien, 16 Cox C.C. 245 (Exch. Div. Ir. 1887) 48, 49

Draper v. United States, 358 U.S. 307 (1959).....44

Dyke v. Taylor Implement Mfg. Co., 391 U.S. 216 (1968).....27

Entick v. Carrington, 95 Eng. Rep. 807 (C.P.), 19 How. St. Tr. 1029 (1765).....49

Fisher v. United States, 425 U.S. 391 (1976).....49

Florence v. Bd. of Freeholders, 132 S. Ct. 1510 (2012).....32

Galatas v. United States, 80 F.2d 15 (8th Cir. 1935) 30, 31

Gouled v. United States, 255 U.S. 298 (1921).....50

TABLE OF AUTHORITIES – Continued

Page

Gracie v. State, 92 So.3d 806 (Ala. Crim. App. 2011) 47

Gustafson v. Florida, 414 U.S. 260 (1973) ..... *passim*

Harris v. United States, 331 U.S. 145 (1947) 14

Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty., 542 U.S. 177 (2004) 32

Hill v. California, 401 U.S. 797 (1971) 50

Illinois v. Lafayette, 462 U.S. 640 (1983) 37

Knowles v. Iowa, 525 U.S. 113 (1998) 21

Kyllo v. United States, 533 U.S. 27 (2001) 57

Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979) 50

Marron v. United States, 275 U.S. 192 (1927) 50

Marsh v. County of San Diego, 680 F.3d 1148 (9th Cir. 2012) 54

Maryland v. King, 133 S. Ct. 1958 (2013) ... 21, 22, 24, 32

Michigan v. DeFillippo, 443 U.S. 31 (1979) 20, 21, 28

Missouri v. McNeely, 133 S. Ct. 1552 (2013) 14, 21

New York v. Belton, 453 U.S. 454 (1981) 18, 19, 20

People v. Blue Cross of California, No. BC492959 (Cal. Super. Ct. Oct. 1, 2012) 53

People v. Bollaert, No. CD252338 (Cal. Super. Ct. Dec. 10, 2013) 42, 53

People v. Chiagles, 237 N.Y. 193 (1923) ..... *passim*

TABLE OF AUTHORITIES – Continued

Page

People v. Citibank, No. RG13693591 (Cal. Super. Ct. Aug. 29, 2013) 53

People v. Custer, 465 Mich. 319 (2001) 45

People v. Diaz, 244 P.3d 501 (2011) 4, 7

People v. Kaiser Foundation Health Plan, No. RG14711370 (Cal. Super. Ct. Jan. 24, 2014) 53

People v. Rivard, 59 Mich. App. 530 (1975) 27

Preston v. United States, 376 U.S. 364 (1964) 27

Shipley v. California, 395 U.S. 818 (1969) 27

Sinclair v. State, 214 Md. App. 309 (2013) 47

State v. Byrd, 178 Wash.2d 611, 310 P.3d 793 (2013) 44

State v. MacDicken, 319 P.3d 31 (Wash. 2014) 45

Thornton v. United States, 541 U.S. 615 (2004) 19, 20, 24, 54

United States v. Aldaco, 477 F.3d 1008 (8th Cir. 2007) 27

United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008) 48, 52

United States v. Barber, 442 F.2d 517 (3d Cir. 1971) 30

United States v. Castro, 596 F.2d 674 (5th Cir. 1979) 44

United States v. Chadwick, 433 U.S. 1 (1977) 17, 18

TABLE OF AUTHORITIES – Continued

Page

United States v. Curtis, 635 F.3d 704 (5th Cir. 2011) 27, 28

United States v. Diaz-Lizaraza, 981 F.2d 1216 (11th Cir. 1993) 45

United States v. Edwards, 415 U.S. 800 (1974) ..... *passim*

United States v. Finley, 477 F.3d 250 (5th Cir. 2007) 28

United States v. Flores-Lopez, 670 F.3d 803 (2012) 34, 36, 39

United States v. Frankenberry, 387 F.2d 337 (2d Cir. 1967) 45

United States v. Grill, 484 F.2d 990 (5th Cir. 1973) 27

United States v. Holzman, 871 F.2d 1496 (9th Cir. 1989), *overruled on other grounds, Horton v. California*, 496 U.S. 128 (1990) 45

United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) 48

United States v. Jones, 132 S. Ct. 945 (2012) 56, 57

United States v. Lynch, 908 F. Supp. 284 (D.V.I. 1995) 45

United States v. McAuley, 563 F. Supp. 2d 672 (W.D. Tex. 2008) 47

United States v. McEachern, 675 F.2d 618 (4th Cir. 1982) 44

United States v. McFarland, II, 633 F.2d 427 (5th Cir. 1980) 45

TABLE OF AUTHORITIES – Continued

Page

United States v. Murphy, 552 F.3d 405 (4th Cir. 2009) 27, 28

United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996) 45

United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003) 33

United States. v. Passaro, 624 F.2d 938 (9th Cir. 1980) 44

United States v. Robinson, 414 U.S. 218 (1973) ..... *passim*

United States v. Rodriguez, 995 F.2d 776 (7th Cir. 1993) 44

United States v. Ross, 456 U.S. 798 (1982) 51

United States v. Smith, 565 F.2d 292 (4th Cir. 1977) 45

United States v. Watson, 669 F.2d 1374 (11th Cir. 1982) 44

United States v. Ziller, 623 F.2d 562 (9th Cir. 1980) 44

Virginia v. Moore, 553 U.S. 164 (2008) 21, 24, 28

Warden v. Hayden, 387 U.S. 294 (1967) 49

Weeks v. United States, 232 U.S. 383 (1914) 10, 48

Welsh v. United States, 267 F. 819 (2d Cir. 1920) 50

Whalen v. Roe, 429 U.S. 589 (1977) 54

TABLE OF AUTHORITIES – Continued

Page

CONSTITUTIONAL PROVISIONS

First Amendment 9, 50

Fourth Amendment ..... *passim*

STATUTES

18 U.S.C. §§ 2510 *et seq* 57

18 U.S.C. §§ 2701 *et seq* 57

OTHER AUTHORITIES

Apple iCloud, Find my iPhone, iPad, and Mac, http://www.apple.com/icloud/find-my-iphone.html (last visited March 31, 2014) 35

California Department of Justice, Bureau of Forensic Services, Physical Evidence Bulletin: Digital Evidence Collection – Mobile Devices 3 (2011), https://oag.ca.gov/sites/all/files/pdfs/cci/reference/peb_18.pdf 40

California Department of Justice, Office of the Attorney General, Privacy Laws, https://oag.ca.gov/privacy/privacy-laws 42

California Department of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013), https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf 42

TABLE OF AUTHORITIES – Continued

Page

Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 Iowa L. Rev. 1125, 1154 (2011) 35

Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 Wm. & Mary Bill Rts. J. 601, 608 (2013) 35, 36

Joint Statement of Principles between California Attorney General and six mobile apps market companies, http://oag.ca.gov/system/files/attachments/press_releases/Apps_signed_agreement_0.pdf#xml=http://search.doj.ca.gov:8004/AGSearch/isysquery/d9cc7c59-4be4-4128-83c3-e93ef6dcc821/1/hilite 42

Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1223 (2004) 57

Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 850-851 (2004) 56

National Institute of Standards and Technology (NIST) SP 800-001, revision 1, *Guidelines on Mobile Device Forensics (Draft); Recommendations of the National Institute of Standards and Technology* 32 (September 2013) http://csrc.nist.gov/publications/drafts/800-101-rev1/draft_sp800_r1.pdf 30, 36, 39

TABLE OF AUTHORITIES – Continued

Page

NIST SP 800-001, *Guidelines on Cell Phone Forensics; Recommendations of the National Institute of Standards and Technology* 34 (May 2007) http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf 34, 38, 39, 40

SC Magazine, Cellebrite UFED Touch Ultimate, http://www.scmagazine.com/cellebrite-ufed-touch-ultimate/review/3870/ (last visited Apr. 1, 2014) 38

Scientific Working Group on Digital Evidence, *for Mobile Phone Forensics, Version 2.0,* at 3 (Feb. 11, 2013) https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%Mobile%20Phone%20Examinations%20V2-0 .....36, 37, 39, 40

Wallen, *Five Apps to Wipe Data from your Android Phone*, TECH REPUBLIC, Feb. 22, 2012; http://www.techrepublic.com/blog/five-apps/five-apps-to-wipe-data-from-your-android-phone/ 35

STATEMENT

1. Petitioner was a member of a San Diego "Blood" gang called "Lincoln Park." On August 2, 2009, he and two other gang members were standing near an intersection when a member of the rival "Crips" gang drove by. Pet. App. 2a. The Bloods fired "numerous shots" at the passing car, causing it to crash. *Id.* They then drove off in a red Oldsmobile, which police later discovered parked a few miles away. *Id.* The Oldsmobile was registered to petitioner, and there was a traffic citation in petitioner's name in the glove compartment. Tr. 723, 854-855.[1]

About three weeks later, petitioner was driving in a different car. San Diego police officer Charles Dunnigan – who was not involved in investigating the earlier shooting, or aware of Riley's involvement in that shooting or his gang affiliation – stopped the car because it had expired registration tags. Tr. 111, 117, 121; J.A. 6-7. When he checked petitioner's license, he discovered that it had been suspended. J.A. 4. Following standard procedures, Dunnigan then decided to impound the car, and an assisting officer conducted a pre-impound inventory search. J.A. 5-6. In the engine compartment, the assisting officer discovered two handguns. Tr. 584-587; J.A. 9. The officers then arrested petitioner for carrying the concealed firearms. Tr. 123-124, 126, 163; J.A. 7-9.

---

[1] "Tr." and "CT" refer to the reporter's transcript and clerk's transcript filed in the court of appeal.

In searching petitioner incident to the arrest, Officer Dunnigan found items suggesting gang membership: a green bandana in petitioner's pocket, and a keychain with a miniature pair of red-and-green Converse shoes. J.A. 8-9. Dunnigan also looked at the cell phone petitioner had in his pocket and noted that text entries starting with a "k" were preceded by a "c," which Dunnigan recognized as a Blood gang symbol (signifying "Crip Killer"). J.A. 8. After finding this evidence of gang affiliation, Dunnigan called Detective Duane Malinowski, of the police department's Gang Suppression Team, to help process petitioner's arrest. J.A. 7, 10, 28.

Detective Malinowski was off-duty that day but came into the station, arriving the same morning. J.A. 15. When he arrived, petitioner was still in the patrol car in the station sallyport. *Id.* Malinowski took petitioner to an interview room; obtained identifying information; read petitioner his rights; ascertained that petitioner did not wish to provide a statement; returned petitioner to the custody of the initial arresting officers; and then "went through [petitioner's] personal property and stuff." J.A. 15-16. Unlike Dunnigan, Malinowski knew petitioner; was familiar with his "infamous reputation in the Lincoln Park street gang"; and suspected him of involvement in the August 2nd shooting. J.A. 16-19.

Detective Malinowski knew that gang members often take pictures of themselves with firearms. J.A. 20. Looking for further evidence to connect petitioner to the firearms found hidden in his car, Malinowski

looked through the photos and videos on the cell phone that had been seized from petitioner during the arrest. *Id.* He did not find pictures of petitioner with the firearms, but he did find video clips of gang members engaged in "street boxing," a common gang initiation. J.A. 11. In the clips, Malinowski could hear petitioner making comments such as "Get brackin', Blood" and "Get him blood. Brack and Blood on Lincoln" – gang terminology encouraging the boxing. J.A. 12-13. There were also photographs showing petitioner and others making gang signs, including the hand sign for the letter "L." J.A. 30-32. Some of the videos and photos on petitioner's phone also showed petitioner's red Oldsmobile. J.A. 12, 30-32.

2. In this case, the State charged petitioner and two others with participating in the August 2 shooting. *See* Pet. App. 1a.[2] As aggravating factors, the State alleged that the offenses were gang-related and involved using firearms. *Id.*

Petitioner moved to suppress evidence found on his cell phone as the fruit of invalid warrantless searches. Tr. 269-270. After an evidentiary hearing, the trial judge denied the motion, concluding that the phone was an item properly seized from petitioner's person, similar to a wallet, purse, or address book, and was validly searched incident to his arrest. J.A.

---

[2] Petitioner separately pled guilty to carrying a concealed firearm in a vehicle, carrying a loaded firearm, and receiving stolen property. Pet. Br. 7 n.5.

23. In particular, she noted Detective Malinowski's testimony that "in his experience persons and gang members do take photos of themselves and their crimes and he expected there could be such photos on the cell phone." *Id.*

The jury at petitioner's first trial could not reach a verdict with respect to petitioner. By the time petitioner was retried, the California Supreme Court had decided *People v. Diaz*, 244 P.3d 501 (2011), upholding a search of the text-message folder of a cell phone as a search incident to arrest. *Id.* at 502. *Diaz* reasoned that the question was controlled by this Court's decisions in *United States v. Robinson*, 414 U.S. 218 (1973) and *United States v. Edwards*, 415 U.S. 800 (1974):

> Under these decisions, the key question in this case is whether defendant's cell phone was "personal property . . . immediately associated with [his] person[,]" like the cigarette package in *Robinson* and the clothes in *Edwards*. If it was, then the delayed warrantless search was a valid search incident to defendant's lawful custodial arrest.

244 P.3d at 505 (citation omitted). The Court concluded that because Diaz's cell phone was found on his person at the time of a lawful arrest, it was properly searched at the police station after the arrest. *Id.* at 505-506, 511. Before petitioner's second trial, the trial court concluded that *Diaz* further supported a ruling that the searches of petitioner's cell phone were lawful incident to his arrest. J.A. 26.

At the second trial, Detective Malinowski testified about materials found on petitioner's phone. J.A. 29-33. He indicated that in one of the video clips on the phone he could see the back portion of petitioner's red Oldsmobile. J.A. 30. He also discussed three photographs that were admitted into evidence as Exhibits 39-41. J.A. 30-31. One photograph shows petitioner standing in front of his Oldsmobile making an "L" shaped sign with his hand, with a fellow Lincoln Park gang member in the background. J.A. 31, 42. The others show the same two individuals by the car making different hand signs. J.A. 31-32, 43-44.

San Diego Police Detective Scott Barnes, a gang expert, testified regarding the Lincoln Park gang and petitioner's membership. *See, e.g.*, J.A. 35-41. Among other things, he explained that the photographs in Exhibits 39-41 showed petitioner and another Lincoln Park gang member, Gerald Haynes, making various gang-related hand signs next to petitioner's car. J.A. 35-36, 38-39, 42-44. Barnes also testified that he had watched videos from petitioner's cell phone showing two Lincoln Park gang members street boxing, with petitioner's car visible in one video, and with audio of petitioner's voice using gang-related terms. J.A. 40-41. None of the videos was admitted into evidence or shown to the jury. Based on his review of the evidence, Barnes opined that petitioner was a member of the Lincoln Park gang. Tr. 1044-1045.

Other evidence at trial showed that the guns found in petitioner's engine compartment were those

used in the August 2 shooting, and that petitioner's DNA was on one of the guns. Tr. 635-640, 943-944. As noted above, the red Oldsmobile used in the shooting was registered to petitioner, and a traffic ticket issued to him was found in the glove compartment. Tr. 723, 854-855. The Police also obtained – using an investigative subpoena, unchallenged in this case – phone company records showing that petitioner's phone had been used near the location of, and around the same time as, the shooting, and several minutes later near where police eventually found the Oldsmobile. Tr. 1008-1012.

The jury also heard recordings of several calls made by petitioner from jail. Tr. 894-900. In one call, petitioner asked an unidentified woman "what exactly did my charges say?" After she said there were "gun charges," he asked, "But did it have – did it have any shooting stuff? It just had gun charges[,] right?" C.T. 237. The woman told petitioner that it only had gun charges and a charge of driving without a license. *Id.* Petitioner asked, "No type of shooting or any. . . ." She said that it had some other "stuff" but that she did not know what it meant. Petitioner said, "it would say like attempted something or something like that." *Id.* In a later call, petitioner said, "like no way that that [stuff], it's gonna come back to me like no matter what, the ballistics, it's gonna show. . . ." C.T. 239. In a third call, petitioner talked about getting bailed out because he knew what was going to "hit eventually." C.T. 242.

The jury found petitioner guilty of assault with a semi-automatic firearm and attempted murder, and that he had personally used a firearm and had committed the offenses for the benefit of a criminal street gang. Pet. App. 1a. The trial court sentenced him to imprisonment for 15 years to life. *Id.*

3. The California Court of Appeal affirmed. Pet. App. 1a-23a. Among other things, it rejected petitioner's renewed claim that evidence admitted at his trial was obtained through improper warrantless searches of his phone. The court reasoned that petitioner's phone "was 'immediately associated' with his 'person' when he was stopped" and that, under this Court's cases and the California Supreme Court's decision in *Diaz*, the searches were lawful incident to petitioner's arrest. *Id.* at 10a-11a, 15a. The California Supreme Court denied petitioner's request for further review. *Id.* at 24a.

SUMMARY OF ARGUMENT

The law has long recognized that it is reasonable for police to search an individual they arrest, and to seize and examine personal effects discovered during such a search. Such searches serve legitimate interests in safety, identification, and securing evidence, and the invasion of privacy involved follows from the arrest itself. These considerations justify searches incident to all valid arrests, both at the scene and later at the police station. This categorical approach

provides clear guidance and a practical rule for operation in the field.

Here, the police properly obtained from petitioner's cell phone the photos and video clips used at his trial. Petitioner does not contest that the phone was properly seized from his person during a valid arrest. It was therefore permissible for the police to examine the phone and its contents as they did, both immediately at the scene and then as part of the ensuing investigation. That conclusion is properly reached under the bright-line rule long applied in similar situations. On the facts of this case, however, the evidence at issue was properly obtained under any potential standard. Examination of videos and photographs on the phone was reasonably related to the officers' investigation of the crime for which petitioner had been arrested; and considerations of safety, identification, and the securing of evidence against possible loss or destruction support the search of petitioner's phone at least as strongly as they have supported searches of other items found on the person of arrestees.

Petitioner argues for a new rule restricting searches of cell phones incident to arrest because of the nature and volume of data they may hold. California recognizes the remarkable advances that have been, and continue to be, made in communications, storage, and networking technology. The facts of this case, however, provide no basis for departure from longstanding Fourth Amendment standards. A phone containing information such as personal communications,

contact information for associates, and the photos and video clips at issue here is not different in kind from wallets, address books, personal papers, or other items that have long been subject to examination by police if carried on the person of an individual who is validly arrested. Nor do the circumstances here raise special First Amendment or other concerns. While technology has increased the amount of information an individual may practically choose to carry, neither the form nor the volume of the information at issue here provides a sound basis for redrawing clearly established Fourth Amendment lines, or reveals any special or unjustified invasion of petitioner's privacy interests.

This case involves photographs and video clips stored on and retrieved from a phone seized in 2009. Nothing about the circumstances here justifies creating new rules treating cell phones such as petitioner's differently from all other items seized from the person of arrestees. The better course is to apply settled principles unless and until some change in conditions produces a result that is manifestly unreasonable on demonstrated facts. Here, the facts reflect only solid police work leading to a sound and just result.

More generally, new technology may affect Fourth Amendment analysis in complex and unforeseeable ways. Continued rapid change is sure; less sure is how and to what extent innovation in digital technology will affect, for example, the accessibility of data stored on phones and its vulnerability to destruction or alteration; the use of phones not only to

store data but to share it in various ways; what steps individuals can readily take to protect data on their phones if they choose; and what data is physically stored on the phone, as opposed to stored elsewhere but available for ready access. Moreover, as these aspects of technology continue to evolve, so may the social expectations relating to them that must be taken into account in determining what is "reasonable" under the Fourth Amendment. All this counsels caution in the judicial formulation of new constitutional rules directed at particular types or categories of devices.

ARGUMENT

I. Under Existing Law, The Police Were Entitled To Search Photos And Videos On Petitioner's Phone As An Incident To His Lawful Arrest

Warrantless searches incident to arrest have long been permitted under the Fourth Amendment, based on the historical practice and understanding that officers conducting a proper arrest may search the person arrested and "seize the fruits or evidence of crime." *Weeks v. United States*, 232 U.S. 383, 392 (1914). The relevant law "has historically been formulated into two distinct propositions" that "have been treated quite differently." *United States v. Robinson*, 414 U.S. at 224. On the one hand, a search "of the *person* of the arrestee" is permitted simply "by virtue of the lawful arrest," *id.*; it "requires no additional justification," *id.* at 235. On the other hand, searches

"of the area within the control of the arrestee" have generated "differing interpretations as to the extent of the area which may be searched." *Id.* at 224. Here, the search of petitioner's cell phone was properly upheld under *Robinson*'s categorical rule, but was also valid even if tested under the rationale of cases involving area searches.

A. The Law Has Long Allowed Police To Search Objects Found On The Person Of An Individual Who Is Lawfully Arrested

1. The leading case on searches of a person incident to a lawful arrest is *United States v. Robinson*, 414 U.S. 218 (1973). There, an officer arrested the defendant for driving with a revoked driver's license. Searching the defendant's pockets, he found a crumpled-up cigarette package. *Id.* at 223. Opening the package, he discovered fourteen capsules of heroin. *Id.* at 223. These were used to convict the defendant of possessing and concealing heroin. *Id.* at 219, 223.

In assessing the constitutionality of this search, *Robinson* observed that the rule allowing warrantless searches incident to a lawful arrest "has historically been formulated into two distinct propositions." *Id.* at 224. First, "a search may be made of the *person* of the arrestee by virtue of the lawful arrest." *Id.* Second, "a search may be made of the area within the control of the arrestee." *Id.* The Court explained that these two types of searches "ha[d] been treated quite

differently." *Id.* Searches of the area surrounding an arrest had been "subject to differing interpretations as to the extent of the area which may be searched." *Id.*; *see* Part I.B, *infra*. In contrast, "[t]he validity of the search of a person incident to a lawful arrest" had been "regarded as settled from its first enunciation," and had "remained virtually unchallenged until the present case." *Id.*

In *Robinson*, the court of appeals reasoned (much as petitioner does here, *see, e.g.*, Pet. Br. 10) that the only two justifications for a search incident to arrest were to disarm the arrestee and to prevent the destruction of evidence of the crime for which the arrest was made. *See* 414 U.S. at 228-229, 233 & n.4. Because "there could be no evidence or fruits" of a revoked-license offense to be found on Robinson's person (*id.* at 233), and because there was no particular reason to fear that Robinson was armed or dangerous (*see id.* at 236 & n.7), the court concluded that the Fourth Amendment permitted no more than a protective frisk incident to the arrest (*id.* at 227, 233).

This Court rejected both that result and the reasoning that underlay it. First, the Court examined the history of searches of the person incident to arrest. It noted that in cases dating back to the 1914 *Weeks* decision (which first adopted a federal exclusionary rule), "no doubt had been expressed as to the unqualified authority of the arresting authority to search the person of the arrestee." *Id.* at 225; *see id.* at 224-226. Similarly, although authorities describing "the history of practice in this country and in

England" were "sparse" and "sketchy," they "tend[ed] to support the broad statement of the authority to search [a person] incident to arrest" found in the Court's prior decisions. *Id.* at 230, 232-235.

Finally, the Court expressed "fundamental disagreement" with the court of appeals' premise that there should be case-by-case litigation concerning the presence or absence of safety or evidentiary concerns sufficient to justify a search of the person of any particular arrestee. It emphasized, instead, the need for a clear, categorical rule to govern police conduct in this common situation, and adopted just such a rule:

> The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect. A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and . . . in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment,

> but is also a "reasonable" search under that Amendment.

Id. at 235; *see also Gustafson v. Florida,* 414 U.S. 260, 266 (1973) (companion case) ("it is the fact of custodial arrest which gives rise to the authority to search"); *Missouri v. McNeely*, 133 S. Ct. 1552, 1559 at n.3 (2013) (recognizing *Robinson*'s adoption of a categorical rule).

Finally, in applying that rule to the facts of the case before it, *Robinson* did not distinguish between a search of the person of the arrestee and a further examination of an object found during that search. Instead, it concluded that, "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it, and when his inspection revealed the heroin capsules, he was entitled to seize them as 'fruits, instrumentalities, or contraband' probative of criminal conduct." 414 U.S. at 236 (quoting *Harris v. United States*, 331 U.S. 145, 154-155 (1947)).

2. Later the same Term, the Court considered a situation in which a further seizure and search of items immediately associated with an arrestee took place some time after the initial arrest. In *United States v. Edwards*, 415 U.S. at 801, officers arrested the defendant for attempting to break into a post office, transported him to the local jail, and held him overnight. Meanwhile, their investigation revealed paint chips near the point of attempted entry. *Id.* In the morning, the officers seized the clothing that

Edwards had been wearing at the time of his arrest, examined it, and found paint chips matching those found at the scene. *Id.* at 802.

Noting the rule the Court had just confirmed in *Robinson* concerning searches incident to custodial arrests, the *Edwards* Court found it "also plain that searches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention." *Id.* at 803. It agreed with prior cases, from this Court and the courts of appeals, that "perceived little difference" between the two situations. *Id.* at 803-804. The ultimate seizure and search, the Court reasoned,

> was and is a normal incident of a custodial arrest, and reasonable delay in effectuating it does not change the fact that Edwards was no more imposed upon than he could have been at the time and place of the arrest or immediately upon arrival at the place of detention. The police did no more on June 1 than they were entitled to do incident to the usual custodial arrest and incarceration.

Id. at 805. Indeed, the Court found it "difficult to perceive what is unreasonable about the police's examining and holding as evidence those personal effects of the accused that they already have in their lawful custody as the result of a lawful arrest." *Id.* at 806. Rather,

> once the accused is lawfully arrested and is in custody, the effects in his possession at the place of detention that were subject to search

> at the time and place of his arrest may lawfully be searched and seized without a warrant even though a substantial period of time has elapsed between the arrest and subsequent administrative processing, on the one hand, and the taking of the property for use as evidence, on the other.

Id. at 807.

Over the years, the principles of *Robinson*, *Gustafson*, and *Edwards* have been applied to a wide variety of items seized from individuals during lawful arrests, including wallets, purses, address books, diaries, other personal papers, pagers, and phones. *See* Parts I.C.1.b and II.A, *infra*.

B. Cases Addressing Searches Of The Area Of An Arrest Have Not Questioned The Categorical Rule Applicable To The Arrestee's Person And Effects

As *Robinson* explained, 414 U.S. at 224, the Court's cases have distinguished between searches of the person of an arrestee, including items found on his person, and those that extend beyond the person to the area in which the arrest is made. In *Chimel v. California*, 395 U.S. 752 (1969), the Court overruled cases that had allowed broad area searches incident to a lawful arrest, instead limiting searches beyond the person to "the area into which an arrestee might reach in order to grab a weapon or evidentiary items." *Id.* at 763; *see id.* at 766-768. Later cases applying *Chimel* have elaborated on that standard for area

searches, notably in the context of arrests made in or near cars. None of those cases, however, has disturbed the categorical rule applicable to items seized from the person of the arrestee.

1. In *Chimel*, officers arrested the defendant in his home and then conducted a warrantless search of the entire home, on the premise that such a search was permitted incident to the arrest. *See id.* at 753-754, 760. Acknowledging that "the decisions of this Court bearing upon that question ha[d] been far from consistent," *id.* at 755, the Court reexamined the issue and concluded that the approval of warrantless searches had extended too far beyond the core case of the arrestee's own person, *see id.* at 755-763. In that core case, the Court reasoned, it was always reasonable to search the arrestee for weapons, and "to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." *Id.* at 762-763. As to the area of the arrest, however, the Court concluded that incidental warrantless searches should extend only to "the area into which an arrestee might reach in order to grab a weapon or evidentiary items." *Id.* at 763.

In *United States v. Chadwick*, 433 U.S. 1, 14-15 (1977), the Court reaffirmed that searches of items found on arrestee's person and in his "'immediate control' area" were always permissible, but declined to extend that rule to a 200-pound, double-locked footlocker that the defendants there had placed in the trunk of a car just before they were arrested. In that situation, the Court reasoned, there was no danger

the defendants could have gained access to the trunk to seize a weapon or destroy evidence; and "[u]nlike [the] searches of the person" involved in *Robinson* and *Edwards*, search of the footlocker "[could not] be justified by any reduced expectations of privacy caused by the arrest." *Id.* at 15-16 & n.10.

Notably, *Chadwick* did not apply to the facts before it the special standards applicable to automobile searches. *Id.* at 11-13. Some years later, however, the Court overruled the result reached on *Chadwick*'s facts (and its application in later cases) in favor of "one clear-cut rule to govern automobile searches," allowing the search of any container found in a car if the police have probable cause to believe it contains contraband or other evidence of crime. *California v. Acevedo*, 500 U.S. 565, 579 (1991); *see id.* at 576-581.

Other discussion of *Chimel* has likewise often come in cases involving cars. In *New York v. Belton*, 453 U.S. 454, 455-457 (1981), for example, the Court considered how *Chimel*'s reachable-area rule should apply to the passenger compartment of a car, when an officer validly arrested the occupants but had already removed them from the car by the time he conducted his search. Citing *Robinson*, the Court emphasized the desirability of "a straightforward rule, easily applied, and predictably enforced." *Id.* at 459. Concluding that items in the passenger compartment of a car would "generally" be within the area reachable by an arrestee, and seeking "to establish the workable rule for this category of cases," the Court held that an officer validly arresting the occupant of a car could

search the passenger compartment as an incident of the arrest. *Id.* at 460. Again citing *Robinson*, the Court made clear that this rule allowed officers to "examine the contents of any containers found" in the passenger area, whether open or closed, and regardless of whether a particular container "could hold neither a weapon nor evidence of the criminal conduct for which the suspect was arrested." *Id.* at 461; *see also id.* ("the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have").

In *Thornton v. United States*, 541 U.S. 615, 617-618 (2004), the Court extended the rule of *Belton* to a situation in which police first made contact with an arrestee just after he had parked and gotten out of his car, and in which the officer had handcuffed the defendant and placed him in the back of a patrol car before searching the passenger compartment of the car. Again stressing the need for clear rules, rather than situation-specific inquiries, the Court held that an officer could search the passenger compartment of a car incident to the arrest of a "'recent occupant.'" *Id.* at 624; *see id.* at 620-624.

More recently, however, the Court has limited *Belton* and *Thornton* to "the rare case," holding instead that "the *Chimel* rationale authorizes police to search a vehicle incident to a recent occupant's arrest only when the arrestee is unsecured and within reaching distance of the passenger compartment at

the time of the search." *Arizona v. Gant*, 556 U.S. 332, 343 & n.4 (2009). At the same time, the Court adopted in part a rule suggested by Justice Scalia's separate opinion in *Thornton*. *Id.* at 343-344. Although the point "does not follow from *Chimel*," the Court "conclude[d] that circumstances unique to the vehicle context justify a search incident to a lawful arrest when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" *Id.* at 343 (quoting *Thornton*, 541 U.S. at 632 (Scalia, J., concurring in the judgment)).

2. All of these post-*Robinson* cases have discussed applications of *Chimel* to objects in the area of an arrest. None of them has questioned the categorical rule of *Robinson* itself, addressing objects on the person of an arrestee. On the contrary, later opinions discussing or adverting to *Robinson* have recognized that, for that situation, *Robinson* expressly adopted a bright-line rule.

In *Michigan v. DeFillippo*, 443 U.S. 31, 35 (1979), the Court cited *Robinson* for just this proposition: "The constitutionality of a search incident to arrest does not depend on whether there is any indication that the person arrested possess weapons or evidence. The fact of a lawful arrest, standing alone, authorizes a search." In *Belton* and *Thornton*, the Court emphasized the same categorical aspect of *Robinson*. *See* 453 U.S. at 459; 541 U.S. at 620. While *Gant* ultimately adopted a different approach for vehicle searches in the recent-occupant context, it nowhere questioned this understanding of *Robinson* as it

applies to searches of the person and any items he is carrying. In *Knowles v. Iowa*, 525 U.S. 113, 118-119 (1998), the Court declined to extend *Robinson* to the context of police issuing citations without making a custodial arrest – but reaffirmed *Robinson*'s adoption, in the arrest context, of "a 'bright-line rule,' which was based on the concern for officer safety and destruction or loss of evidence, but which did not depend in every case upon the existence of either concern." Likewise, in *Virginia v. Moore*, 553 U.S. 164, 176-177 (2008), the Court again emphasized the categorical nature of the *Robinson* rule: "The interests justifying search are present whenever an officer makes an arrest. . . . The state officers *arrested* Moore, and therefore faced the risks that are 'an adequate basis for treating all custodial arrests alike for purposes of search justification.'" *Id.* at 177 (quoting *Robinson*, 414 U.S. at 235).

Just last Term, the Court again cited *Robinson* as an example of the "limited class of traditional exceptions to the warrant requirement that apply categorically and thus do not require an assessment of whether the policy justifications underlying the exception . . . are implicated in a particular case." *Missouri v. McNeely*, 133 S. Ct. at 1559 n.3. Finally, in *Maryland v. King*, 133 S. Ct. 1958, 1970-1971 (2013), the Court approvingly quoted both *Robinson*'s own observation that "'[t]he validity of the search of a person incident to a lawful arrest has been regarded as settled from its first enunciation, and has remained virtually unchallenged,'" and *DeFillippo*'s

restatement of *Robinson*'s bright-line rule. *See also id.* at 1978 (noting that "unlike . . . a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy," and quoting *Edwards* for the proposition that "'both the person [of an arrestee] and the property in his immediate possession may be searched at the station house'" (alterations changed)).

C. The Evidence At Issue Here Was Properly Obtained Under Any Standard

The Court's cases have thus established a categorical rule permitting arresting officers to seize and search items of personal property found on the person of an arrestee – either at the time and place of an initial arrest or within a reasonable time thereafter. Cases addressing search and seizure of items in the *area* of an arrest have focused instead on whether the object was found in a place where the arrestee might have reached to grab a weapon or destroy evidence – with a special rule, in the context of vehicle passenger compartments, that police may freely search for evidence of the crime of arrest. Finally, some justices have suggested that if the rationale for a search is the discovery or preservation of evidence, it should be limited to a scope reasonably related to the crime of arrest, or perhaps other crimes already known or suspected. Under the circumstances of this case, the proper rule is the categorical one of *Robinson* and *Edwards*. In any event, however, the photographic

and video evidence used at petitioner's trial was properly obtained under any of these standards.

1. The photos and videos were found in searches of an object recovered from petitioner's person during his arrest

San Diego police properly searched petitioner's cell phone, both at the scene of the initial arrest and later when petitioner had been brought to the police station, because petitioner was carrying the phone on his person at the time he was arrested for carrying loaded firearms concealed in his car. *See* Pet. Br. 4. Only after the lawful arrest did Officer Dunnigan first examine petitioner's cell phone and see that some entries starting with a "k" were preceded by a "c," indicating a gang affiliation. J.A. 8. Not long thereafter, a detective specializing in gang activity, who had been called to the police station to assist with the arrest, further reviewed photo and video files on the phone. That examination revealed materials that were later used at trial. Under *Robinson* and *Edwards*, these searches were properly performed incident to petitioner's arrest, and were categorically reasonable under the Fourth Amendment.

a. That result is compelled by precedent, and by the long tradition the precedent reflects. *See, e.g.*, *Robinson*, 414 U.S. at 224-225; *Edwards*, 415 U.S. at 802-804; *see also Gustafson*, 414 U.S. 267 (Stewart, J., concurring) ("To hold otherwise would . . . mark an abrupt departure from settled constitutional

precedent."). But both the tradition and the precedent are also based on reason and common sense.

First, as the Court has observed, the interests in officer safety and in safeguarding evidence "are present whenever an officer makes an arrest." *Moore*, 553 U.S. at 177. Second, even if that point might be argued in marginal cases, where police are making custodial arrests any argument for case-by-case evaluation is overwhelmed by the general probabilities, the importance of the interests at stake, and the need for clear guidance. *See, e.g.*, *Thornton*, 541 U.S. at 632 (Scalia, J., concurring in the judgment) ("When officer safety or imminent evidence concealment or destruction is at stake, officers should not have to make fine judgments in the heat of the moment."); *id.* at 626 ("Authority to search the arrestee's own person is beyond question."). Third, in making an arrest the police have a compelling interest in ascertaining or verifying the identity of the arrestee, *see, e.g.*, *Maryland v. King*, 133 S. Ct. at 1971-1972 (citing cases), which is likely to be best served in the first instance by examining items found on the individual's person. Fourth, the safety, evidentiary, and identification purposes of a search of the person could not be effectively served if officers were allowed to seize items but not examine them. *See, e.g.*, *People v. Chiagles*, 237 N.Y. 193, 197 (1923) ("The search being lawful, [an officer] retains what he finds if connected with the crime."); *cf. id.* at 198 ("Search would be mere futility if what is found could not be used.").

Finally, and in part for these very reasons, the mere fact of a lawful custodial arrest necessarily and substantially reduces the arrestee's expectation of privacy, as to his own person and as to any personal property in his immediate possession – not perhaps as against the world, but as against the arresting officers and those legitimately called on to help investigate a crime. *See, e.g.*, *Robinson*, 414 U.S. at 235 ("A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification."). As explained by Justice Powell, concurring in *Robinson* and *Gustafson* (414 U.S. at 237), "the custodial arrest is the significant intrusion of state power into the privacy of one's person. If the arrest is lawful, the privacy interest guarded by the Fourth Amendment is subordinated to a legitimate and overriding governmental concern." Or, as the Court put it in *Edwards*, a lawful arrest takes a person's privacy, to a reasonable extent, "'out of the realm of protection from police interests in weapons, means of escape, and evidence.'" 415 U.S. at 808-809.

b. Petitioner argues at some length that, even if these normal rules would have applied to petitioner's cell phone at the initial scene of his arrest, Detective Malinowski's examination of the phone at the police station was too remote in time and place to be approved. Pet. Br. 44-53. That is not correct.

Examination of petitioner's phone at the station was just as routine an incident of his arrest as a

search at the initial scene. Indeed, it occurred while the arrest was still being processed. *See* pp. 2-3, *supra*. As this Court explained in *Edwards*, "searches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention." 415 U.S. at 803. Of course, for safety reasons, some search of an arrestee will almost always be made immediately. But once the search of both the person and any objects he is carrying has been made reasonable by the fact of the arrest, it is hard to see the benefit, in terms of either privacy or practicality, of insisting that every aspect of the search take place at once, or at the initial scene. In particular, that scene will often be a busy street or highway, or in a public setting that may be difficult to monitor or control, or dark, or exposed to bad weather. While convenience or efficiency often cannot justify burdening rights, in this situation there is no incremental burden. *See Edwards*, 415 U.S. at 805-806 (arrestee is "no more imposed upon" by delayed search than was justified by initial arrest, and "[i]t is difficult to perceive what is unreasonable about the police's examining and holding as evidence those personal effects of the accused that they already have in their lawful custody as the result of a lawful arrest").

That is especially true where, as here, an item is first examined at the original scene. Where items have once "been exposed to police view under unobjectionable circumstances, . . . no reasonable expectation of privacy is breached by an officer's taking a

second look at matter with respect to which [the] expectation of privacy already has been at least partially dissipated." *United States v. Grill*, 484 F.2d 990, 991 (5th Cir. 1973); *see also, e.g.*, *People v. Rivard*, 59 Mich. App. 530, 533-534 (1975) (same); *United States v. Aldaco*, 477 F.3d 1008, 1013-1016 (8th Cir. 2007) (second look at wallet). The Fourth Circuit has expressly applied this reasoning to a cell phone search: "Of course, once the cell phone was held for evidence, other officers and investigators were entitled to conduct a further review of its contents, as [the agent] did, without seeking a warrant." *United States v. Murphy*, 552 F.3d 405, 412 (4th Cir. 2009).

In arguing for a more restrictive rule, petitioner cites cases from this Court that mostly predate *Edwards* and are, in any event, inapposite, dealing with the different question of searches of the area where an arrest is made. *See* Pet. Br. 44-46; *Shipley v. California*, 395 U.S. 818, 819-820 (1969) (search of home when defendant arrested outside); *Preston v. United States*, 376 U.S. 364, 367 (1964) (search of car at storage yard after arrest); *Dyke v. Taylor Implement Mfg. Co.*, 391 U.S. 216, 220 (1968) (search of car at police station). He also cites four unpublished decisions from lower courts dealing with cell phone searches – three from district courts and one from a state appellate court. Pet. Br. 44 & n.15. Notably, he does not cite three published appellate decisions upholding searches of phones seized during arrests but searched at least in part later. *See United States v. Curtis*, 635 F.3d 704, 712 (5th Cir. 2011) (search of

text messages at the scene and later at Secret Service office); *Murphy*, 552 F.3d at 412 (search of phone numbers at scene and later at station); *United States v. Finley*, 477 F.3d 250, 260, n.7 (5th Cir. 2007) (search of phone after arrestee transported for questioning). At a minimum, a search remains "incident to an arrest for 'as long as the administrative processes incident to the arrest and custody have not been completed.'" *Curtis*, 635 F.3d at 712. That describes Detective Malinowski's examination of petitioner's phone while petitioner was being booked. *See* pp. 2-3, *supra*.

2. The searches here were reasonably related to the crime of arrest

As discussed above, this Court's cases have not limited the permissible scope of examination of an object found on an arrestee's person by reference to the crime of arrest. *Robinson*, 414 U.S. at 233; *Gustafson*, 414 U.S. at 265; *Moore*, 553 U.S. at 170; *DeFillippo*, 443 U.S. at 35-36. The Court has looked to whether officers could reasonably have believed they might find evidence relevant to the crime of arrest only as an alternative justification for searches of the passenger compartment of a car, even if a recent occupant has been secured and is not within reaching distance of the compartment at the time of his arrest. *See Gant*, 556 U.S. at 343-344, 346-347. To the extent the question is relevant, however, in this case there were reasonable grounds to believe that reviewing photographs and video clips on petitioner's phone

would lead to evidence relevant to the firearms offense for which he had been arrested.

As part of his job, Detective Malinowski monitored activity involving the Lincoln Park gang, and was familiar with petitioner's "infamous reputation" in that gang. J.A. 16; Tr. 852. Malinowski also knew, based on his training and experience, that gang members often record evidence of their crimes on their phones. J.A. 20. Accordingly, he believed petitioner's phone might contain videos or photographs further linking petitioner to the firearms that had been hidden in his car. J.A. 20. In denying petitioner's motion to suppress, the trial court expressly referenced Malinowski's testimony that, in examining petitioner's phone, he was looking for evidence connecting petitioner with the guns found in the car. J.A. 23. Accordingly, there is no question that Malinowski's search was objectively justified by a reasonable likelihood that it would lead to evidence of the crime for which petitioner had been arrested.

3. A cell phone such as petitioner's presents safety, identification, and evidentiary issues at least as powerful as those relating to other items routinely seized and searched incident to arrest

Finally, even if the Court were to consider whether the general rationales underlying searches incident to arrest apply in the specific circumstances here (*but see, e.g.*, *Robinson*, 414 U.S. at 235), examination of

petitioner's phone was at least as well justified as the search of other items found on the person of an arrestee.

a. Safety and identification

First, petitioner is wrong to say (Br. 10) that "the digital contents of a smart phone are categorically incapable of threatening officer safety." On the contrary, "[m]obile devices may be rigged to detonate bombs remotely or explode themselves if a specific action is carried out on the device (e.g., receiving an incoming call, text message or pressing a specific key chord sequence, etc.)." National Institute of Standards and Technology (NIST) SP 800-001, revision 1, *Guidelines on Mobile Device Forensics (Draft); Recommendations of the National Institute of Standards and Technology* 32 (September 2013) (*NIST Draft Guidelines*).[3] Moreover, a phone (including any non-voice communication capabilities) could obviously be used, either openly or surreptitiously, to summon assistance from confederates who could interfere with an arrest and pose a direct threat to officers and the public. *Cf., e.g., United States v. Barber*, 442 F.2d 517, 520-521 (3d Cir. 1971) (fifteen men assaulted two federal agents who were attempting to take arrestee to their vehicle, allowing escape); *Galatas v. United States*, 80 F.2d 15, 19-20 (8th Cir. 1935) ("Pretty Boy"

---

[3] *Available at* http://csrc.nist.gov/publications/drafts/800-101-rev1/draft_sp800_101_r1.pdf.

Floyd's ambush of federal agents as they transported escaped gang member back to prison). Indeed, with modern technology, an arrestee would not necessarily even need to make active use of a phone in order for confederates to use its signals to locate, track, and potentially aid him. A phone such as petitioner's on the person of an arrestee can thus pose a threat to both officer and public safety.

Petitioner argues that police may serve their interests by searching for and seizing a phone, which he concedes is permissible, but not examining the phone's "digital contents." Pet. Br. 10; *see id.* at 16-19. But without inspecting an item – including a phone – police cannot even know whether it *is* of either safety or evidentiary concern. *See, e.g.*, *Chiagles*, 237 N.Y. at 198-199 (complaining that neither defendant nor prosecutor informed court of contents of letters seized from defendant's person during arrest, so court could not determine whether police had properly retained them). Without examining a phone, police cannot tell whether it has been "weaponized," or whether officers should summon help because, for example, the arrestee contacted a confederate shortly before the arrest; arranged to meet others at or near the time and place of the arrest; or even arranged a crime that is about to occur.

Moreover, examining a phone (but not simply seizing it) may assist an arresting officer in rapidly confirming or calling into question the identity of an arrestee – a matter of immediate concern "in every criminal case," and one about which arrestees have

been known to provide false or incomplete information to officers in the field. *Maryland v. King*, 133 S.Ct. at 1971 (quoting *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 191 (2004)). And apart from the identity of the arrestee himself, inspection may reveal links to criminal associates – including, as here, association with a dangerous criminal gang. All of these issues relate directly to officer, public, and even arrestee safety. *Cf. Florence v. Bd. of Freeholders*, 132 S. Ct. 1510, 1518-1519 (2012) ("the identification and isolation of gang members before they are admitted [into custody] protects everyone in the facility.").

In any event, the line between seizing an object from the person of an arrestee and examining it to determine its significance is not one the Court has drawn in the past, nor one it should draw now. Officers who seize a gun from an arrestee, for example, need not obtain a warrant before examining it to determine whether it is loaded, or with what type of ammunition, or whether there is a readable serial number or other identifying information, or to perform ballistics testing, or to make any other evidentiary examination. Officers who search an arrestee and find packages of what appear to be illegal drugs need not obtain a warrant before testing them to confirm or refute that suspicion. The ordinary and sensible principle is, instead, that "[h]aving in the course of a lawful search come upon" an item, officers "are entitled to inspect it." *Robinson*, 414 U.S. at 236; *see also Edwards*, 415 U.S. at 806. As Justice Cardozo

put a similar point for the New York Court of Appeals, "the law would be flouted and derided if, defeating its own ends, it drew too fine a point, after sanctioning the search, between the things to be retained and the things to be returned." *Chiagles*, 237 N.Y. at 197. And without examination, one cannot even know which is which.

b. Preservation of evidence

A cell phone is also at least as subject to the potential destruction of important evidence as other items routinely subject to seizure and search incident to an arrest. If anything, the case for seizure and prompt inspection for purposes of evidentiary preservation is stronger for a modern cell phone than for more traditional items such as the cigarette packages in *Robinson* and *Gustafson*, the clothes in *Edwards*, or a wallet, diary, address book, letter, account book, or the like.

1. To begin with, the information on a phone is readily susceptible to alteration or erasure by an arrestee. With a few hand motions, the entire contents of a device might be deleted, or rendered inaccessible with a password or encryption that could be difficult or impossible to defeat.

Moreover, even if the phone has been removed from the arrestee's immediate reach, the data on the phone, or the ability to gain access to or use the data, may remain at risk. On some phones, for example, new incoming calls or messages might replace old data. *United States v. Parada*, 289 F. Supp. 2d 1291,

1304-1305 (D. Kan. 2003). In addition, phones often have limited battery life, and a loss of power may result in a loss of content. As the National Institute of Standards and Technology (NIST) notes, "[i]f user data resides in battery-dependent volatile memory, expiration of the battery would be disastrous." NIST SP 800-001, *Guidelines on Cell Phone Forensics; Recommendations of the National Institute of Standards and Technology* 34 (May 2007) (*NIST Guidelines*).[4] And some data may have to be reviewed quickly or lose its investigative or evidentiary usefulness. *See, e.g.*, *United States v. Flores-Lopez*, 670 F.3d 803, 810 (2012) (if conspirators buy prepaid "SIM" cards and replace them frequently, an "officer who seizes one of the cell phones will have only a short interval within which to discover the phone numbers of the other conspirators").

A phone may also be protected with mechanisms such as a password. A phone that is password-protected may lock automatically, often after a relatively short period, if not in active use. If an arrestee was using a phone at the time of arrest, or had recently used it, arresting officers have no way of knowing if the mere passage of a short period of time will cause a lock to activate, thereby blocking access without entry of a password. Depending on the type of phone, such a lock could effectively thwart law enforcement efforts to view the contents of the phone at

---

[4] *Available at* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

any later time – even with a warrant. While some protection mechanisms can be bypassed, others likely cannot, or cannot without resources far beyond the reach of any ordinary criminal investigation.

The data on a phone may also be subject to automatic or remote destruction. Users can, for example, program some phones to self-erase after a certain number of failed access attempts. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 Iowa L. Rev. 1125, 1154 (2011). Applications such as Snapchat, Wickr, and Tiger Text are specifically designed to erase data after a certain period of time. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 Wm. & Mary Bill Rts. J. 601, 608 (2013). And "remote wipe" applications – typically marketed as a means of protecting data in the case a phone is lost or stolen – can allow anyone with proper codes and wireless access to the device to erase the contents of the phone. *E.g.*, Wallen, *Five Apps to Wipe Data from your Android Phone*, TECH REPUBLIC, Feb. 22, 2012; *see also* Apple iCloud, Find my iPhone, iPad, and Mac.[5] "[R]emote-wiping capability is available on all major cell-phone platforms; if the phone's manufacturer doesn't offer it, it can be

---

[5] Wallen, *supra*, is available at http://www.techrepublic.com/blog/five-apps/five-apps-to-wipe-data-from-your-android-phone/; Information on the Apple application is at http://www.apple.com/icloud/find-my-iphone.html (last visited Mar. 31, 2014).

bought from a mobile-security company." *Flores-Lopez*, 670 F.3d at 808. Thus, even if a phone is removed from the possession of an arrestee, either the arrestee or a confederate, with access to a computer or other phone and wireless connection to the seized device, could destroy data on the device after the arrest. Indeed, with foresight, an arrestee could program some phones to erase all user data if the phone's geo-location system determines that it has either left or entered a predetermined geographical area – such as, for example, the area around a local police station. *NIST Draft Guidelines* 3.

2. Petitioner seeks to deflect these concerns by arguing that officers could take various steps to preserve data while they seek a warrant. Pet. Br. 20-24. These might include using another device to copy the phone's contents, or taking some step designed to stop it from receiving or sending signals – turning it off, removing a data card, accessing the phone only for purposes of placing it in "airplane mode," placing it in a "Faraday enclosure," wrapping it in aluminum foil, or using a radio jamming system. *Id.* at 22-24; *see, e.g.*, Gershowitz, *supra*, 22 Wm. & Mary Bill Rts. J. 601; Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Mobile Phone Forensics, Version 2.0*, at 3 (Feb. 11, 2013) (*SWGDE Best Practices*).[6]

---

[6] *Available at* https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20V2-0.

Of course, the question in this case is whether the search that was conducted was reasonable – not whether the police might also have served their purposes through some other, arguably less-intrusive means. *See, e.g.*, *Illinois v. Lafayette*, 462 U.S. 640, 647-648 (1983); *Edwards*, 415 U.S. at 807 ("[i]t was no answer to say that the police could have obtained a search warrant, for the Court held the test to be, not whether it was reasonable to procure a search warrant, but whether the search itself was reasonable, which it was" (describing *Cooper v. California*, 386 U.S. 58, 62 (1967)). But even on their own terms, petitioner's arguments do not justify prohibiting a prompt examination of a phone's contents when arresting officers conclude that is the best way to proceed.

First, petitioner's arguments depend on current technology. Particularly in the present context, that is not a sound basis for framing Fourth Amendment rules. "New families of mobile phones are typically manufactured every three (3) to six (6) months. Many of these phones are closed operating systems and proprietary interfaces making it difficult for the forensic extraction of digital evidence." *SWGDE Best Practices* 3. Given the wide variety of phone manufacturers and operating systems and the rapid pace of change, petitioner's arguments can provide no basis for confidence that arresting officers will be able to maintain the status quo with respect to phone data.

Second, none of these measures can reliably meet the legitimate needs served by the decisions that arresting officers may make, under particular circumstances, to proceed with a prompt examination of a phone's contents. *See, e.g.*, *NIST Guidelines* 34.

Data extraction devices, for example, are both too cumbersome and too expensive for the Constitution to require that they be carried by every officer who is likely to find a cell phone while making an arrest – or even that they be available at every local station house.[7] Moreover, even sophisticated devices may well be unable to retrieve data from a modern phone if a password lock or encryption system has been allowed to engage.

Attempts to block signals in or out of the phone have similar shortcomings. Placing a phone in "airplane mode," for example, sounds simple, but in any given situation it may or may not be possible, depending on the phone; may or may not block all signals on a given phone; and in any event requires officers to interact with the phone, which may or may not be familiar to them, and which they may or may not

---

[7] For instance, the Cellebrite UFED Touch Ultimate, a mobile forensic tool allowing data acquisition from more than 8,000 mobile devices, starts at $10,000, which does not include the cost of annual updates. SC Magazine, Cellebrite UFED Touch Ultimate, http://www.scmagazine.com/cellebrite-ufed-touch-ultimate/review/3870/ (last visited Apr. 1, 2014).

want to access immediately, depending on the particular circumstances of an arrest. Likewise, Faraday bags or other enclosures are hardly the panacea that petitioner suggests. Although they are less expensive than data extraction devices, it remains both unrealistic and inappropriate to argue that the Constitution requires every potential arresting officer to carry one or more Faraday bags at all times or risk losing potentially significant evidence. *See Flores-Lopez*, 670 F.3d at 810.

In any event, Faraday devices do not reliably block all incoming signals. *NIST Guidelines* 34; *NIST Draft Guidelines* 32 ("The majority of test cases proved that the shielding devices tested did not prevent network communication in all cases. . . ."). They do not prevent a password or encryption system from activating and blocking further access. And they can quickly drain a phone battery, causing the phone to turn itself off and further risking permanent loss of the ability to retrieve data. *NIST Guidelines* 38 ("Because communications are blocked, the handset continues increasing its signal strength up to the maximum as it continually attempts to make contact. This activity significantly shortens battery life."); *SWGDE Best Practices* 3 ("Blocking [radio frequency] signals will drain the battery, may be expensive, [is] not always successful and may result in the alteration of mobile phone data."). If power is drained from the phone then volatile memory, which is used for dynamic storage, could be permanently lost. *NIST*

Guidelines 43. And when a phone is powered back on, more difficult encryption or blocking mechanisms may have been engaged. *SWGDE Best Practices* 4 ("Many mobile phones may lose data or initiate additional security measures once discharged or shut down."); *NIST Draft Guidelines* 31.

Citing California guidelines, petitioner maintains that police departments across the country have been using Faraday bags for several years. Pet. Br. 23. He fails to mention, however, that those guidelines expressly caution about the power-draining consequences of that approach. Cal. Dep't of Justice, Bureau of Forensic Servs., Physical Evidence Bulletin: Digital Evidence Collection – Mobile Devices 3 (2011) ("If you place a powered 'ON' cellular phone in a Faraday bag, the device should be examined as soon as possible because the battery will drain during this period, and will turn off."; in such circumstances, officer must "[d]ocument any data that is transmitted to the device (i.e., incoming calls, text messages, etc.) during seizure, and record all information present on the screen.").[8]

In any event, the point is not that police use of Faraday bags or similar measures is never appropriate. Clearly it may be. The point is that the Constitution does not require officers in the field to

---

[8] *Available at* https://oag.ca.gov/sites/all/files/pdfs/cci/reference/peb_18.pdf.

choose one of those methods of proceeding whenever they find a cell phone on the person of a suspect during an arrest. Instead, one potential method of proceeding that will always be *reasonable* – and thus constitutionally permissible – for officers who discover an unlocked phone is to conduct their own prompt search. From the Fourth Amendment perspective, that approach is at least as well justified in the case of personal cell phones as it has been in previous cases involving other types of personal property.

II. The Technological Advances That Petitioner Highlights Do Not Warrant The Adoption Of Special Rules For Cell Phones In This Case

Fundamentally, petitioner argues that the development of modern cell phones is an "innovation [that] gives law enforcement the ability to obtain personal information formerly beyond its reach," requiring a change in the Fourth Amendment rules previously applicable to searches of items seized from an individual's person during the course of a lawful custodial arrest. Pet. Br. 13-14; *see id.* at 24-37. The Constitution's protections, he insists, "should not evaporate . . . simply because . . . information can now be reduced to electronic charges in a computer chip and carried in one's pocket." *Id.* at 12.

California recognizes the remarkable and rapidly continuing advance of communication, data storage,

and networking technologies, and the privacy concerns that these developments raise or sharpen in many situations. Indeed, California has been a leader on privacy issues, such as seeking to protect personal information from improper acquisition, disclosure, or other misuse – either by the cyber-criminals who have developed in tandem with the new technologies, or by commercial service providers or other third parties to whom individuals may disclose information, sometimes without a full appreciation of the possible consequences, in the course of using attractive new technologies.[9]

Here, however, petitioner's concerns are misplaced. As discussed above, where an individual is properly arrested, the law has long recognized that the arrest itself both entails and justifies a substantial invasion of the individual's privacy – not

---

[9] *See, e.g.*, https://oag.ca.gov/privacy/privacy-laws (citing California's Constitutional and legislative privacy protections); *People v. Bollaert*, No. CD252338 (Cal. Super. Ct. Dec. 10, 2013) (prosecution of operator of website that published explicit photographs without authorization and extorted payment from victims for removal); California Department of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013), *available at* https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (providing recommendations to assist mobile application developers and others in considering privacy in the application and implementation of applications); Joint Statement of Principles between California Attorney General and six mobile apps market companies (2012), *available at* http://oag.ca.gov/system/files/attachments/press_releases/Apps_signed_agreement_0.pdf#xml=http://search.doj.ca.gov:8004/AGSearch/isysquery/d9cc7c59-4be4-4128-83c3-e93ef6dcc821/1/hilite.

necessarily as against the world, but as against those responsible for the investigation of crime. Contrary to petitioner's submission, the photographs and video clips found on petitioner's phone when he was arrested are not fundamentally different from, or more sensitive than, other types of personal information long carried by individuals in non-digital forms. The question is not whether petitioner should receive *less* Fourth Amendment protection because he carried his information in digital instead of paper form, but rather whether he should receive *more*. At least on the facts of this case, neither changes in the way that information may be stored nor the resulting increase in the volume of information that an individual may choose to carry justifies any alteration in the legal standards long applicable to custodial arrests. The facts here reveal only sound, traditional police work, albeit involving a modern technology. They provide no basis for any change in the law.

A. The Information Taken From Petitioner's Phone Is Not Fundamentally Different From That Found In Other Searches Incident To Arrest

Much of petitioner's argument proceeds from his assertion that information found on cell phones – such as "text, photo, and video files," calendars, contact lists, bank or health records, or business information (*see* Pet. Br. 27) – is fundamentally different from the sort of information that police might have discovered in previous searches of individuals during

arrests. There is, however, little basis for that contention in the facts of this case or of others that have come before the courts.

1. Although this Court has considered only a few factual scenarios in articulating the Fourth Amendment standards for searches of the person incident to arrest, the lower courts have been applying those standards for many years. The searches approved in these cases have often involved items containing sensitive personal information fundamentally *similar* to that now carried on phones, such as wallets or purses, diaries, papers, address books, and pagers.

Arrest searches often include, for example, wallets and their contents. *See, e.g., United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993) ("the search of Rodriguez's wallet and the photocopying of the contents of the address book were permissible as a search incident to arrest"); *United States v. McEachern*, 675 F.2d 618, 622 (4th Cir. 1982); *United States v. Watson*, 669 F.2d 1374, 1383-1384 (11th Cir. 1982) (wallet and papers within); *United States. v. Passaro*, 624 F.2d 938, 944 (9th Cir. 1980); *United States v. Ziller*, 623 F.2d 562, 563 (9th Cir. 1980); *United States v. Castro*, 596 F.2d 674, 677 (5th Cir. 1979) (wallet and folded piece of paper inside wallet containing list of locations to deliver marijuana). In appropriate circumstances, purses or hand luggage have likewise been subject to search. *See Draper v. United States*, 358 U.S. 307, 310 (1959) (noting that items were seized both from arrestee's hand and from a bag he was carrying); *State v. Byrd*, 178 Wash.2d

611, 310 P.3d 793, 797-798 (2013) (purse was "'immediately associated' with [arrestee's] person"); *State v. MacDicken*, 319 P.3d 31, 34 (2014) (laptop bag carried on person and rolling duffel bag "immediately associated" with arrestee); *Curd v. City Court of Judsonia, Arkansas*, 141 F.3d 839, 844 (8th Cir. 1998). All these items can contain papers and other personal information similar to the information often carried on phones.

Likewise, papers found in the pockets of an arrestee may be examined by an officer as part of a search incident to arrest. *United States v. McFarland, II*, 633 F.2d 427, 429 (5th Cir. 1980); *Chiagles*, 237 N.Y. at 197-199. This includes an address book, diary, or photograph found on the arrestee's person. *United States v. Diaz-Lizaraza*, 981 F.2d 1216, 1220, 1223-1224 (11th Cir. 1993) (wallet and address book, including loose papers); *United States v. Holzman*, 871 F.2d 1496, 1504-1505 (9th Cir. 1989), *overruled on other grounds, Horton v. California*, 496 U.S. 128 (1990); *United States v. Smith*, 565 F.2d 292, 294 (4th Cir. 1977) (address book in pocket of arrestee's coat); *United States v. Frankenberry*, 387 F.2d 337 (2d Cir. 1967) (diary); *cf. People v. Custer*, 465 Mich. 319, 324-325, 334-338 (2001) (photographs obtained during pat-down search). And since the early 1990s, courts have applied the same principles to digital information stored in personal electronic devices such as pagers. *See, e.g., United States v. Ortiz*, 84 F.3d 977 (7th Cir. 1996); *United States v. Lynch*, 908 F. Supp. 284, 288-289 (D.V.I. 1995) ("Since a search of the

'person' has been held to include a person's wallet or address book, we find that a search of Thomas' pager was a search of his 'person' and thus was valid[.]").

Thus, *Robinson* and *Edwards* have been applied to uphold searches of personal items seized from arrestees containing just the sorts of personal information that many individuals now store and carry on their phones – identification, contact information for associates, photographs, papers relating to business (including criminal business), and recent communications. Of course, these searches invade important personal privacy interests. They have been upheld, however, because they occur in the context of valid arrests.

Cell phones represent an evolution in the means individuals use to carry information on their persons, and in the amount they can easily carry at one time. But information such as the photographs and video clips involved in this case is not different in kind from what the law has dealt with for many years.

Far from being material that individuals previously "kept . . . – if it existed in tangible form at all – only in the most private recesses of their homes and offices" (Pet. Br. 11), much of the information now stored on phones is routine material that individuals have long recorded, stored in various places, and often carried on their persons in other forms for ready reference. Digital storage technology simply makes it easy for individuals to keep more of such information with them much of the time – often so that it can be

readily available for use in daily activities or to share with others, for purposes either good or ill. Thus, "'[d]igital files and programs on cell phones have merely served as replacements for personal effects like address books, calendar books, photo albums, and file folders previously carried in a tangible form.'" *Sinclair v. State*, 214 Md. App. 309, 330 n.14 (2013) (quoting *Gracie v. State*, 92 So.3d 806, 812 (Ala. Crim. App. 2011)); *see id.* ("There is little question that if the photographs [found on the defendant's cell phone] were found in a wallet at the time, they would not be suppressed."); *United States v. McAuley*, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008) (search of laptop computer at border; "The fact that a computer may take such personal information and digitize it does not alter the Court's analysis."). That development may have advantages and disadvantages, including with respect to both the preservation of privacy and the facilitation of crime. But, at least so far as the type of information involved in this and similar cases is concerned, it is not a qualitative change that demands the creation of new Fourth Amendment rules.

2. Nor is there any basis for treating petitioner's phone differently from other property seized from an arrestee simply because it might contain information that "implicates First Amendment concerns." *See* Pet. Br. 25, 31-36. That is true of any message, photograph, recording, text, contact list, or business

paper that might be seized in either digital or tangible form.[10]

Petitioner nowhere cites this Court's 1914 decision in *Weeks*, which provided the starting point for *Robinson*'s consideration of searches of objects found on the person of an arrestee. *See* 414 U.S. at 224-225. Notably, however, when *Weeks* observed that English and American law had "always recognized" an ability "to search the person of the accused when legally arrested, to discover and seize the fruits or evidence of crime," 232 U.S. at 392, it relied in part on *Dillon v. O'Brien*, 16 Cox C.C. 245, 250 (Exch. Div. Ir. 1887). That reliance confirms that there is no special rule for "private papers" of the sort petitioner suggests (*e.g.*, Pet. Br. 32).

In *Dillon*, the Irish Court of the Exchequer traced the common-law right of constables to detain as evidence property found during an arrest. Dillon was arrested in a room with co-conspirators, receiving rents from tenants and making entries in books and papers to reflect the receipts. The arresting officers also seized the books and papers, among other items. 16 Cox C.C. at 247, 248. The court considered it

---

[10] Arguments similar to petitioner's have been rejected in the context of border searches of laptop computers. *See United States v. Ickes*, 393 F.3d 501, 506-507 (4th Cir. 2005) (First Amendment exception to border search doctrine would be unworkable and have "staggering" implications; terrorists' communications, for example, are "inherently 'expressive' "); *United States v. Arnold*, 533 F.3d 1003, 1010 (9th Cir. 2008).

indisputable that officers making a felony arrest could "take and detain property found in [the arrestee's] possession which will form material evidence in his prosecution for that crime." *Id.* at 249. In applying the same principle to misdemeanors, the court distinguished *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P.), 19 How. St. Tr. 1029 (1765), on which petitioner relies (Pet. Br. 32). It reasoned that papers were seized from Dillon not under a general warrant or on mere suspicion, "but upon an allegation of actual guilt, and a lawful apprehension of the guilty person." *Dillon*, 16 Cox C.C. at 251; *see also id.* (in *Entick*, "Lord Camden had not before his mind cases of seizure of evidences of guilt upon lawful apprehension, as distinguished from general warrants to seize all papers"); *Chiagles*, 237 N.Y. at 197 (distinguishing *Entick* as involving search to discover possible grounds for arrest, not search of person during valid arrest).

Petitioner points out (Br. 32, 34 n.11) that in *Boyd v. United States*, 116 U.S. 616, 630-634 (1886), this Court cited *Entick* and generally condemned searches for "private papers" to be used as evidence of crime. *Boyd*, however, has "not stood the test of time." *Fisher v. United States*, 425 U.S. 391, 407, 409 (1976). Even as to personal papers, there is no Fourth Amendment distinction between purely evidentiary materials and contraband or fruits or instrumentalities of crime. *Warden v. Hayden*, 387 U.S. 294, 300 (1967); *Fisher*, 425 U.S. at 409. Indeed, this Court and others have long recognized that "[t]here is no special

sanctity in papers, as distinguished from other forms of property, to render them immune from search and seizure, if only they fall within the scope of the principles of the cases in which other property may be seized." *Gouled v. United States*, 255 U.S. 298, 309 (1921); *see, e.g., Marron v. United States*, 275 U.S. 192, 198-199 (1927) (ledger and bill lawfully seized incident to arrest); *Hill v. California*, 401 U.S. 797, 800 & n.1, 806-807 (1971) (two pages of diary properly searched incident to arrest); *see also, e.g., Chiagles*, 237 N.Y. at 196 (letters); *Welsh v. United States*, 267 F. 819, 821 (2d Cir. 1920) (letter).

Petitioner wrests cases from their contexts in analogizing the cell phone search here to one subject to special rules relating to "expressive materials." Pet. Br. 33; *see Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326-327 (1979) (specifically noting that case involved "a generalized search under authority of an invalid warrant," not a search incident to arrest). Any such rules surely cannot depend on the nature of the device or medium in which particular information may be stored. A photograph, short video, letter, list of addresses, or other material that could be properly seized from an arrestee's pocket in paper form is not imbued with special First and Fourth Amendment protection simply because it is digitized and carried on a cell phone.

B. The Circumstances Of This Case Suggest No Basis For Specially Limiting Cell Phone Searches Incident To Arrests

Other concerns that petitioner raises, apart from the basic nature of the information that may now be stored on a phone, likewise do not warrant creating any special rule to govern searches of cell phones seized from the persons of arrestees, at least on the facts of this case.

1. Petitioner argues that cell phones can store "massive amounts" of information. Pet. Br. 26; *see, e.g.*, *id.* at 26-28. But it is not clear how mere storage capacity relates to the concerns protected by either the Fourth Amendment or the rule permitting searches of items seized from the person of an arrestee. Examination of conventional items (wallets, letters, photographs, address books) can reveal private information – in particular, information that the carrier would strongly prefer to keep private from the police. Conversely, a cell phone may contain a great deal of information of no interest to the police. It is not necessarily an advantage to law enforcement that a criminal who might previously have carried one or two needles can now bring along an entire haystack. Moreover, it would be inappropriate to allow some individuals to shield themselves from standard searches because they are solvent and well-advised enough to carry evidence of their misdeeds in electronic rather than paper form. *Cf. United States v. Ross*, 456 U.S. 798, 822 (1982) (no distinction between "worthy"

and "unworthy" containers). Neither the particular form in which data is stored and carried (digital or tangible) nor the storage capacity of a particular device seems a sound basis for drawing Fourth Amendment lines.[11]

Petitioner's comparisons to general-warrant searches and police "rummag[ing]" through phones (*e.g.*, Br. 3, 26) also overstate the concerns raised by the present case. First, although the phone in this case was not password-protected, for reasons discussed above there is reason to doubt how often police will have the practical ability to access information on seized phones – at least as password and encryption technology advances, and where the phone's owner actually views the information with the degree of sensitivity that petitioner suggests. In any event, even where data is readily available for review, officers who search a phone will typically be looking first for anything that indicates an immediate safety threat, and then for any information that confirms a suspect's identity or provides useful evidence of crime. Normally they will have a particular focus, such as the crime of arrest, in mind – as Detective Malinowski did here. *See* pp. 2-3, 26-27, *supra*.

---

[11] As with petitioner's other arguments, a similar contention that laptop computers "allow[ ] for the storage of personal documents in an amount equivalent to that stored in one's home" has been rejected in the context of border searches. *United States v. Arnold*, 533 F.3d at 1006.

While officers may well see other information in the course of an examination, most of it will be both of no interest to the officers and innocuous in itself. Moreover, exposure to private information that turns out to be unrelated to crime is commonplace for police officers. While it is no doubt good practice to minimize that exposure where possible, it is important to recognize that a limited review of private information by police in the course of an investigation is not equivalent to other compromises of informational privacy that can give rise to particular concerns in the digital context – theft by hackers, for example, or inadvertent or malicious disclosure of private information to the general public.[12] Where police officers review otherwise private information, even in the context of a warrantless search, they do so for a legitimate purpose; and if the information is *not* relevant to safety or to investigating or preventing crime, their use of the information ends without further disclosure. Disclosure to the police is not disclosure to the world.[13]

---

[12] *See, e.g., People v. Bollaert, supra*, No. CD252338 (Cal. Super. Ct. Dec. 10, 2013); *People v. Kaiser Foundation Health Plan*, No. RG14711370 (Cal. Super. Ct. Jan. 24, 2014) (untimely notification of data breach); *People v. Citibank*, No. RG13693591 (Cal. Super. Ct. Aug. 29, 2013) (same); *People v. Blue Cross of California*, No. BC492959 (Cal. Super. Ct. Oct. 1, 2012) (public disclosure of social security numbers).

[13] Petitioner points to one case apparently involving wrongful dissemination of irrelevant private photographs obtained during a search of an arrestee's phone. Br. 37 n.12. California does not condone any such behavior. Legal rules cannot, however, be

(Continued on following page)

None of this is to deny that police inspection of a phone's contents, to the extent it is possible, impinges on important privacy interests. Here, however, as in any other case involving an object seized from an individual during an arrest, "it is the fact of custodial arrest which gives rise to the authority to search"; the arrest itself being lawful and having already substantially interfered with the individual's privacy as well as his liberty, the related search "requires no additional justification." *Robinson*, 414 U.S. at 235-236; *see also, e.g.*, *id.* at 260 (Powell, J., concurring). Indeed, even where a search extends *beyond* items found on the arrestee's person, "[t]he fact of prior lawful arrest distinguishes the arrestee from society at large, and distinguishes a search for evidence of *his* crime from general rummaging." *Thornton*, 541 U.S. at 630 (Scalia, J., concurring). The search in this case was aimed at discovering photographic evidence linking petitioner to the firearms he had been arrested for possessing. It in fact disclosed evidence of

---

framed to avoid any possible misconduct. *Cf. Whalen v. Roe*, 429 U.S. 589, 601-602 (1977). Nor is there any reason to think that requiring a warrant to search cell phones seized during arrests would prevent any similar misuse of information obtained during an authorized search. In contrast, existing remedies apply to the misuse of information gained by any means. *See, e.g.*, *Catsouras v. Department of the California Highway Patrol*, 181 Cal. App. 4th 856, 863-907 (2010) (tort liability for wrongful dissemination of crime scene photographs); *Marsh v. County of San Diego*, 680 F.3d 1148 (9th Cir. 2012) (release of autopsy photograph to press without legitimate government purpose violated substantive due process).

his gang affiliation, and further linked him to a gang-related shooting that was also under investigation. It involved no unreasonable invasion of petitioner's privacy interests.

2. One aspect of modern phone technology that may be genuinely new is its heavily networked nature – that is, the potential not only for storing personal information but for sharing, changing, and accessing it remotely through interaction with other devices. Again, however, the possible Fourth Amendment implications of this development are far from clear.

One result of networking is that information stored on a phone is far more susceptible to alteration or loss than would be true with non-networked objects. As discussed above (at 43-49), this supports the continued application of current law allowing for prompt law enforcement searches. Another result is the common use of phones both to store data that is also stored in other places and to *share* data, including both text and images – sometimes publicly, or at least very widely. A third, closely related, result is the routine disclosure of information, including some that may otherwise be thought of as quite private, to a variety of intermediaries, including communications companies and other service providers. A fourth is that phones can be used not only to store data but to access or manipulate data that is primarily stored elsewhere – although the access most likely involves storing at least temporary copies of the accessed material on the phone itself.

All these aspects of evolving phone technology could have implications for the Fourth Amendment analysis of particular situations – including by altering the general social expectations that undergird at least some of that analysis. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."). Furthermore, the technology itself continues to evolve – rapidly, and in ways that are often hard to imagine before they occur.

All this counsels judicial caution in formulating the sort of new, categorical, technology-specific constitutional rule that petitioner seeks in this case. If there is a need for specific rules to address specific technologies, that task is best left to legislatures, which are better able "to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *see also* Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 850-851 (2004) ("courts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new

technologies").[14] Courts should strive, instead, "to apply existing Fourth Amendment doctrine," asking whether "a particular case involved a degree of intrusion that a reasonable person would not have anticipated." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

In this case, there is no question concerning government deployment of some new technology to monitor private behavior that was previously undetectable as a practical matter. *Cf. Jones*, 132 S. Ct. at 949 (attaching GPS device to monitor vehicle's movements, even through public spaces, was a "search" subject to the Fourth Amendment); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (use of thermal imaging to measure heat emanating from home was a Fourth Amendment search). The arrest here was made on wholly traditional grounds, after officers properly looked under the hood of a car and discovered dangerous weapons stashed in socks. Tr. 584-587; J.A.

---

[14] Congress has, for example, extensively addressed the question of electronic communications. *See generally* 18 U.S.C. §§ 2510 *et seq.*, 2701 *et seq*. This includes copies of information often found on personal phones, such as emails, texts, images, or other data that has already been disclosed to third parties providing communications services. Notably, investigators typically may obtain much of this information with administrative subpoenas or court orders, sometimes without notice to the subscriber, based on less than the showing of probable cause that petitioner would require for examination of a cell phone seized from an individual during an arrest. *See, e.g., id.* § 2703; Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1223 (2004).

7-9. The officers' ensuing examination of petitioner's cell phone was a conventional search, authorized by longstanding precedent. A reasonable person in petitioner's position would have anticipated at least this level of intrusion into his privacy interests based on the fact of his lawful arrest.

Indeed, the course of events in this case reflects only solid, traditional, effective police work, leading to a just conviction. The circumstances here suggest no occasion for any change in Fourth Amendment law.

CONCLUSION

The judgment of the California Court of Appeal should be affirmed.

Respectfully submitted,

KAMALA D. HARRIS
Attorney General of California
EDWARD C. DUMONT
Solicitor General
DANE R. GILLETTE
Chief Assistant Attorney General
JULIE L. GARLAND
Senior Assistant Attorney General
STEVE T. OETTING
CRAIG J. KONNOTH
Deputy Solicitors General
CHRISTINE M. LEVINGSTON BERGMAN
Deputy Attorney General
Counsel of Record

Dated: April 2, 2014

REPLY BRIEF

RECORD AND BRIEFS

No. 13-132

Supreme Court, U.S.
FILED
APR 22 2014
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari
to the California Court of Appeal,
Fourth Appellate District

REPLY BRIEF FOR PETITIONER

Patrick Morgan Ford
LAW OFFICE OF PATRICK MORGAN FORD
1901 First Avenue
Suite 400
San Diego, CA 92101

Donald B. Ayer
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001

Jeffrey L. Fisher
Counsel of Record
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@law.stanford.edu

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

REPLY BRIEF FOR PETITIONER 1

I. The Fourth Amendment Prohibits Searching The Digital Contents Of Smartphones Incident To Arrest 2

A. *Robinson* Does Not Confer A Categorical Authority To Search Smartphones 2

B. No Governmental Interest Requires A Categorical Authority To Search Smartphones Incident To Arrest 8

1. Officer Safety 8

2. Preserving Evidence 9

3. Identification 15

C. None Of The State's Or The United States' Attempts To Mitigate The Implications Of Their Positions Is Persuasive 16

II. The Search Of Petitioner's Phone At The Stationhouse Was Too Remote From His Arrest To Qualify As A Search Incident To Arrest. 22

CONCLUSION 24

APPENDICES

Appendix A 1a

Appendix B 2a

Appendix C 3a

TABLE OF AUTHORITIES

Page(s)

CASES

California v. Acevedo, 500 U.S. 565 (1991) 7

Chimel v. California, 395 U.S. 752 (1969).....2, 3, 7, 11

Dillon v. O'Brien & Davis, 16 Cox C.C. 245 (Exch. Div. Ir. 1887) 7

Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).....19

Gouled v. United States, 255 U.S. 298 (1921).....6

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) 15

In re Search of an Apple I-Phone Model A1332, No. 1:12-mj-304 (W.D. Mich. Oct. 9, 2012) 17

Knowles v. Iowa, 525 U.S. 113 (1998) 2

Marron v. United States, 275 U.S. 192 (1927).....6

Maryland v. King, 133 S. Ct. 1958 (2013).....3, 15, 16

Mincey v. Arizona, 437 U.S. 385 (1978) 24

Missouri v. McNeely, 133 S. Ct. 1552 (2013) 4, 14

Newell v. State, 49 So. 3d 66 (Miss. 2010) 14

People v. Blanchette, 2014 WL 718414 (Cal. Ct. App. 2014).....12

People v. Villasana, 2010 WL 7122 (Cal. Ct. App. 2010).....14

Schmerber v. California, 384 U.S. 757 (1966).....3, 4

Shipley v. California, 395 U.S. 818 (1969) 22

Thornton v. United States,
541 U.S. 615 (2004) 9, 18, 19, 23

United States v. Burnette, 698 F.2d 1038
(9th Cir. 1983) 24

United States v. Chadwick, 433 U.S. 1 (1977) 8

United States v. Edwards,
415 U.S. 800 (1974) 3, 22, 23

United States v. Fricosu, 841 F. Supp. 2d 1232
(D. Colo. 2012) 15

United States v. Gavegnano, 305 Fed. Appx. 954
(4th Cir. 2009) 15

United States v. Jones, 132 S. Ct. 945 (2012) 5, 19

United States v. Karo, 468 U.S. 705 (1984) 5

United States v. Kirschenblatt, 16 F.2d 202
(2d Cir. 1926) 7

United States v. Knotts, 460 U.S. 276 (1983) 5

United States v. Nyuon, 2013 WL 1339713
(D.S.D. 2013) 14

United States v. Robinson,
414 U.S. 218 (1973) ..... *passim*

United States v. Stevens,
130 S. Ct. 1557 (2010) 16, 17

United States v. Williams, 2014 WL 412526
(D. Vt. 2014) 14

United States v. Wurie, 728 F.3d 1
(1st Cir. 2013) 10

Virginia v. Moore, 553 U.S. 164 (2008) 2

CONSTITUTIONAL PROVISIONS

U.S. Const., amend. IV ..... *passim*

U.S. Const., amend. V 15

OTHER AUTHORITIES

Apple, iOS Human Interface Guidelines (2014) 21

Ayers, Rick, *et al.*, National Institute of Standards and Technology, U.S. Dept. of Commerce, Guidelines on Mobile Device Forensics (Draft) (Sept. 2013) 9, 10, 13

Brynjolfsson, Erik & Andrew McAfee, The Second Machine Age (2014) 6

California District Attorneys Association, Cell Phone Records Training Materials, Advanced Asset Forfeiture Update Course (March 16-18, 2010) 15

Catholic Church Gives Blessing to iPhone App, BBC (Feb. 8, 2011) 18

Katta, Sahas, *How My Smartphone Got Me Out of a Speeding Ticket in Traffic Court*, Skatter Tech (Feb. 21, 2011) 19

McCullagh, Declan, *How Apple and Google Help Police Bypass iPhone, Android Lock Screens*, CNet (April 2, 2012) 15

Schmidt, Eric & Jared Cohen, The New Digital Age (2013) 6

Specs, Samsung Galaxy S5 (2014) 13

REPLY BRIEF FOR PETITIONER

The State maintains that anytime a police officer arrests a person for any offense, the police department should be automatically entitled to conduct an unbounded, warrantless search of the person's smartphone. According to the State, precedent commands such a wide-ranging and absolute authority, and it is necessary to serve various law enforcement interests.

But this Court's holding in *United States v. Robinson*, 414 U.S. 218 (1973), does not mandate the categorical ruling the State seeks. That decision was issued before the advent of smartphones – devices increasingly necessary to navigate innumerable tasks of daily life and on which people now carry the entirety of their private papers in their pockets or purses. Nor do any of the law enforcement interests the State identifies support the rule it seeks. These interests merely show that in certain isolated situations, exigent circumstances may justify inspecting smartphones before warrants could reasonably be obtained.

That leaves the State's and the United States' attempts to mitigate the dramatic implications of the power they seek. The State's suggestion that this Court simply leave it to legislatures, police officers, or future cases to limit the scope of smartphone searches is unconvincing. And the United States' various fallback positions either fail to meaningfully curb the authority it requests or would be entirely unworkable. The decision below should be reversed.

I. The Fourth Amendment Prohibits Searching The Digital Contents Of Smartphones Incident To Arrest.

A. *Robinson* Does Not Confer A Categorical Authority To Search Smartphones.

The State argues that when the police seize a smartphone from an arrestee's person, this Court's holding in *United States v. Robinson*, 414 U.S. 218 (1973), mandates that officers have a categorical right – irrespective of the factors outlined in *Chimel v. California*, 395 U.S. 752 (1969) – to explore the smartphone's digital contents. Resp. Br. 10-11. This argument overreads *Robinson*.

1. In *Robinson*, this Court explained that, just like the authority to search an arrestee's grab area, the authority to search an arrestee's person is "based upon the need to disarm and to discover evidence." 414 U.S. at 235; *see also id.* (*Chimel* justifications are "the reasons supporting the authority for a search of the person incident to a lawful arrest"). Subsequent cases say the same. *See, e.g.*, *Virginia v. Moore*, 553 U.S. 164, 176 (2008) (officers may search arrestee's person "in order to ensure their safety and safeguard evidence"); *Knowles v. Iowa*, 525 U.S. 113, 118 (1998) (same).

Robinson simply held that when it comes to purely physical items on an arrestee's person, one or both of the *Chimel* justifications is so likely, if not inherently, present that case-by-case adjudication is unwarranted. *See Robinson*, 414 U.S. at 235; *see also Chimel*, 395 U.S. at 763 (same with respect to grab area). *Robinson* did not consider – nor could it have –

whether the same reasoning applies to digital data on a smartphone.

2. The State responds that *Robinson* nevertheless confers the categorical authority it seeks because this Court's opinion notes that when an item is seized from an arrestee's person, "the mere fact of a lawful custodial arrest" reduces an arrestee's expectation of privacy in the item. Resp. Br. 25; *see also* U.S. Br. 8-9 (stressing same point).[1] But nothing about this reality creates a categorical power, untethered from *Chimel*, to search smartphones.

a. While an arrest diminishes an arrestee's expectation of privacy in his person, "the mere fact of a lawful arrest does *not* end our inquiry." *Schmerber v. California*, 384 U.S. 757, 769 (1966) (emphasis added). That is, not every search of an arrestee's personal effects "is acceptable solely because a person is in custody." *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013). Such searches "must [still] be tested by the Fourth Amendment's general proscription against unreasonable searches." *United States v. Edwards*, 415 U.S. 800, 808 n.9 (1974). Accordingly, when searching an arrestee involves categorically "greater intrusions or higher expectations of privacy," then the privacy-related concerns may be "weighty enough that the search may require a warrant." *King*, 133 S. Ct. at 1979.

Indeed, for just these reasons, the Court has long deemed the authority described in *Robinson* inapplicable to one type of search of an arrestee's

---

[1] Unless otherwise noted, references are to the United States' brief in this case, not *United States v. Wurie*, No. 13-212.

person. Notwithstanding the language in historical materials describing an "unrestricted" right to search the persons of arrestees, this Court has held that when police wish to search beneath the body's surface, Fourth Amendment privacy interests require the police, absent exigent circumstances, to seek a warrant. *Schmerber*, 384 U.S. at 769-70; *see also Missouri v. McNeely*, 133 S. Ct. 1552, 1564, 1559 n.3 (2013) (recognizing that *Robinson* is inapplicable in the context of drawing blood incident to arrest). The question here, therefore, is not whether this Court should create an exception to some preexisting, absolute authority to search the persons of arrestees, but rather – as in *Schmerber* – whether it is reasonable to extend the authority described in *Robinson* to a new kind of search that prior generations could never have envisioned.

b. It would be unreasonable to render the mere fact of an arrest sufficient cause for police to conduct a warrantless, exploratory search of an arrestee's smartphone. A smartphone holds exponentially greater amounts of sensitive information than any physical item an arrestee could carry on his person. Smartphones accordingly implicate the Fourth Amendment's core prohibition against general warrants in a way that searching physical items cannot. *See* Petr. Br. 29.

The State resists this analogy, protesting that digital information on smartphones – while admittedly more voluminous – "is not different in kind from what the law has [allowed to be searched incident to arrest] for many years." Resp. Br. 9, 46; *see also* U.S. Br. 22 (same argument). This argument bears a striking resemblance to the position the

Government unsuccessfully advanced in *United States v. Jones*, 132 S. Ct. 945 (2012). It is even less persuasive here.

In *Jones*, the United States marshaled two cases, *United States v. Karo*, 468 U.S. 705 (1984) and *United States v. Knotts*, 460 U.S. 276 (1983), purportedly establishing a categorical rule that people lack any reasonable expectation of privacy in movements through public areas. The Government then argued that "although GPS technology is more advanced than the beeper technology" used in those cases, this technological advance was irrelevant because "it reveals the same type of information" as beepers do. U.S. Reply Br. 1, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259). Not one Justice agreed with this argument, and five squarely rejected it. As Justice Alito explained, the "practical" capability of GPS technology to aggregate information in a manner unforeseeable to prior generations rendered the privacy implications different not just in degree but in kind. *Jones*, 132 S. Ct. at 963-64 (concurring in judgment); *see also id.* at 956 (Sotomayor, J., concurring).

So too here. Searching a smartphone is different in kind than searching any purely physical object that might be seized from an arrestee – even something like a wallet or spiral notebook. As numerous *amici* elaborate, smartphones contain truly massive quantities of information – "the equivalent of [carrying in one's pocket] the cabinets, desks, bookshelves, and bureaus in an eighteenth century home," Br. of ACLU 6, as well as one's entire office, library, *see* Br. of Am. Library Ass'n 13-15, random thoughts and wonders, and collections of medical,

financial, and consumer records. *See also* Br. of NACDL 3-6. Furthermore, smartphones contain not merely more information, but new types of information (such as GPS-locational information and real-time physiological data) different from anything a person carried in the days of purely analog belongings.[2] With each passing year, the smartphone will only become more of a nerve center for our daily activities, relationships, and very identities. *See, e.g.*, Erik Brynjolfsson & Andrew McAfee, The Second Machine Age 34 (2014); Eric Schmidt & Jared Cohen, The New Digital Age 13-59 (2013).

Contrary to the State's insistence (Resp. Br. 47-50), the expressive nature of the virtual warehouses of information on smartphones only accentuates the privacy stakes involved. The State cites several old cases supposedly establishing a historical indifference to searching private papers incident to arrest. But the State's cases establish merely that officers could historically seize papers, just like non-expressive items, when they were "instruments" of the crime of arrest. *Gouled v. United States*, 255 U.S. 298, 309-10 (1921); *see also Marron v. United States*, 275 U.S. 192, 199 (1927) (papers were

---

[2] For example, Samsung's latest phones contain heart-rate monitors. Smartphone apps can sync with Fitbits – small monitoring devices worn on the wrist – to collect and store a user's sleep patterns and calories burned. *See Fitbit*, http://www.fitbit.com/flex. Smartphones will also soon be used to "keep track of your blood pressure, detect nascent heart disease[,] identify early-stage cancer" and "monitor [] insulin levels." Eric Schmidt & Jared Cohen, The New Digital Age 25 (2013).

"actually used to commit the offense"); *Dillon v. O'Brien & Davis*, 16 Cox C.C. 245, 247 (Exch. Div. Ir. 1887) (papers were "being used for the purpose of such combination and conspiracy"). Indeed, in *United States v. Kirschenblatt*, 16 F.2d 202 (2d Cir. 1926) – the very case the United States quotes for the supposedly absolute principle that "the law has never distinguished between documents and other property found upon the person of one arrested" – Judge Hand stressed that seizing a few papers that are instrumentalities of crime is fundamentally different from "rummag[ing] at will among [an arrestee's] papers in search of whatever will convict him." *Id.* at 203, quoted in U.S. Br. 6, 26. Allowing the latter – he believed and other historical sources demonstrate – would "countenance exactly what the amendment was designed to prevent." *Id.* at 204; *see also* Petr. Br. 31-32, 34-36.

c. Finally, distinguishing as sharply as the State would between smartphones seized from a person's pocket and phones seized from an arrestee's immediate vicinity would be irrational. This Court has stressed that Fourth Amendment rules "must not turn on . . . coincidences" or mere happenstance. *California v. Acevedo*, 500 U.S. 565, 580 (1991). Partly for this reason, *Chimel* itself emphasized that searches of persons and the area into which an arrestee might reach "must, of course, be governed by a like rule." 395 U.S. at 763. Given that a smartphone is just as likely to be in an arrestee's pocket as sitting nearby in her briefcase or on her desk, such an extraordinary privacy interest should not be dependent on whether the arrestee is holding the phone at the moment of apprehension or whether it is sitting inches away.

B. No Governmental Interest Requires A Categorical Authority To Search Smartphones Incident To Arrest.

None of the State's arguments about officer safety, destruction of evidence, or identifying arrestees satisfies *Chimel*'s standard for allowing categorical warrantless searches incident to arrest. At the very most, the State imagines a few isolated scenarios that would trigger the exigent circumstances doctrine.

1. Officer Safety

a. *Bombs.* The State posits that smartphones can be used as (or to trigger) bombs. Resp. Br. 30. This scarcely resonates as an everyday concern. If ever it does arise, this Court has already held that "if officers have reason to believe that [a seized item] contains some immediately dangerous instrumentality, such as explosives," the exigent circumstances doctrine allows officers to search it immediately. *United States v. Chadwick*, 433 U.S. 1, 15 n.9 (1977). The State offers no reason why the same would not be true here.

b. *Confederates.* The State also hypothesizes that arrestees might use smartphones "to summon assistance from confederates." Resp. Br. 30. But even though cell phones have been in widespread use for over a decade, the State fails to cite a single instance, over tens of millions of arrests, in which one has ever been used to do this. Crediting a possibility so "remote in the extreme" to allow blanket authority for searches incident to arrest would stretch "current doctrine . . . beyond its breaking point." *Thornton v. United States*, 541 U.S. 615, 625 (2004) (Scalia, J., concurring in judgment). As with a possible bomb, if

officers really think that an arrestee may have summoned an ambush, exigent circumstances would permit inspection of the phone.

2. Preserving Evidence

The State also contends that warrantless searches incident to arrest are necessary to prevent digital data from being remotely wiped or rendered forever inaccessible behind personal security features. Once again, neither of these arguments justifies the categorical authority the State seeks.

a. *Remote wiping.* Contrary to the State's contentions, simple steps that officers already take on a daily basis allay any concern that a phone might be remotely wiped.

As an initial matter, it is customary for officers first to put seized smartphones in airplane mode. *See* Rick Ayers et al., National Institute of Standards and Technology, U.S. Dept. of Commerce, Guidelines on Mobile Device Forensics (DRAFT) 36-37 (Sept. 2013) ("NIST Draft Guidelines").[3] The State complains that this "requires officers to interact with the phone." Resp. Br. 38. But triggering airplane mode is much easier than doing something else the State confidently reports that officers can do: search throughout a phone while taking care not to alter or delete any of its contents. It takes only one or two clicks in a phone's settings (regardless of whether it is locked) to put it in airplane mode. *See* Appendix A. And while the State muses that airplane mode "may

---

[3] http://nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

not block *all* signals," Resp. Br. 38 (emphasis added), it does completely block remote wiping commands. *See* NIST Draft Guidelines 30.

If for some reason an officer is unable or unwilling to put a phone in airplane mode, Faraday bags are "simple and inexpensive security techniques" that also block remote wiping commands. Br. of EPIC 5. The State responds that Faraday bags may not work forever because they "depend on current technology." Resp. Br. 37. But all smartphones for the foreseeable future will operate via radio waves, and those are what Faraday bags block. If an entirely new basis for smartphone technology someday emerges, this Court could then "revisit this issue." *See United States v. Wurie*, 728 F.3d 1, 13 n.12 (1st Cir. 2013).

The State next notes that Faraday bags "can quickly drain a phone battery." Resp. Br. 39. Yet as any smartphone user can attest, a phone does not lose any perceptible information if its battery dies. This is because smartphones, like other modern computers, keep most everything in permanent storage. The State's suggestion (*id.* at 34) that a phone might lose "content" if its battery dies cites a manual published in 2007, before smartphone technology emerged.[4]

---

[4] The only information the State or United States identifies that might be lost if a *modern* phone's battery dies is an "encryption key." Resp. Br. 40; U.S. Br. 12. But an encryption key matters only if password protection threatens to preclude officers from gaining access to information on a device. For the reasons described in the next subsection, this concern is not at issue here and is highly unlikely to arise in other cases.

Finally, the State argues that Faraday bags "do not reliably block all incoming signals." Resp. Br. 39. It may be true, at least in laboratory settings, that some Faraday bags occasionally let bits of radio waves through. But the proof of the pudding is in the eating: Officers routinely use Faraday bags, *see* Br. of Crim. Law Profs. 4-6, and neither the State nor its *amici* can point to a single instance of a seized phone that was placed in a Faraday bag ever being remotely wiped.[5] Whatever the odds of this occurring someday, they surely pale in comparison to the possibility that "confederates of [a man arrested in his home] will in the meanwhile remove the items for which the police have probable cause to search." *Chimel*, 395 U.S. at 774 (White, J., dissenting). Yet even that potential danger is insufficient to justify warrantless examinations of arrestees' entire homes incident to arrest. *See id.* at 763.

b. *Password protection.* Raising an argument never advanced before the merits briefing in this Court – and, indeed, seemingly never raised previously in *any* appellate proceeding – the State and the United States contend that officers need to "prompt[ly]" search smartphones insofar as passwords might prevent them "at any later time –

---

[5] This reality also disposes of the United States' suggestion that even if a phone is placed in a Faraday bag, any previously blocked remote wiping command could execute as soon as the phone is removed, U.S. Br. 16. Again, the Government offers no evidence of this ever happening. If airplane mode is somehow unavailable and remote wiping is a genuine concern, the police can transport the phone to a signal-proof environment before removing it from the bag.

even with a warrant" from accessing the phones' digital contents. Resp. Br. 33-35; *accord* U.S. Br. 11.

This argument does not apply to the facts of this case. Petitioner's smartphone "was not password-protected." Resp. Br. 52. The photos and videos at issue were stored on a removable memory card which would have been accessible even if the phone had been locked. Petr. Br. 22; *see also, e.g.*, *People v. Blanchette*, 2014 WL 718414, at *2 (Cal. Ct. App. 2014) (describing how police were able to view photos on a password-protected device simply by ejecting the memory card). And the phone was not searched until two hours after its seizure, long after police knew it was not going to lock.[6]

What is more, the State's password-protection argument depends on numerous factual premises that make the concern the State hypothesizes so unlikely to arise that it could not possibly justify the categorical authority the State seeks:

- For starters, the police would have to seize a phone "in an unlocked state." U.S. Br. 13. Yet a phone will not be unlocked unless it has been used within minutes of an arrest. And even then, a user need only press a single button to re-lock the phone. So officers will rarely recover a phone in an unlocked state.

---

[6] The United States suggests that an iPhone's auto-lock feature could suddenly kick in after as much as "four hours." U.S. Br. 11. Not so. The maximum delay is five minutes. *See* Appendix C. The United States references the potential time period before *password protection* kicks in, which does not start running until a phone has already locked.

- If the phone is unlocked, the police would have to be incapable of easily discerning whether the phone is password-protected. Yet an officer need only press a couple of buttons under "settings" to find out whether this is the case. *See* Appendix B.
- If an unlocked phone is indeed password-protected, the police would have to be unable to disable the phone's "auto-lock" feature to prevent the password from kicking in. Yet that too requires pressing only a few buttons. *See* Appendix C.
- The police also would have to want to examine content that is capable of being password-protected. Many phones, including petitioner's and some current Android models, store some or all of their data on memory cards that are accessible regardless of any password-protection.[7]
- The police would have to be unable to ensure future access to the unlocked phone's contents by connecting it to another device, such as a laptop in a police cruiser. Yet according to the NIST Draft Guidelines (at 35), taking this step creates a "trusted relationship" that will "ensure that the data can be accessed at a later time, after the device is locked."
- Lastly, the police would have to be unable to guarantee future access to content on an

---

[7] *See, e.g.*, *Specs*, Samsung Galaxy S5 (2014), http://www.samsung.com/global/microsite/galaxys5/specs.html.

> unlocked phone that is protected by a password simply by asking the owner at the scene for the password. Yet cases demonstrate that this tactic is often successful. *See, e.g.*, *United States v. Williams*, 2014 WL 412526, at *4 (D. Vt. 2014); *United States v. Nyuon*, 2013 WL 1339713, at *3 (D.S.D. 2013); *People v. Villasana*, 2010 WL 7122, at *1 (Cal. Ct. App. 2010); *Newell v. State*, 49 So. 3d 66, 71 (Miss. 2010). Indeed, if refusing to divulge a password could expose one's unlocked phone to a warrantless exploratory search, most individuals presumably would much rather divulge the password for use if the police secure a particularized warrant.

If and when this collection of prerequisites ever comes to pass, then seizing an unlocked phone might give rise to exigent circumstances justifying an immediate warrantless search. *See McNeely*, 133 S. Ct. at 1561. This depends on whether law enforcement is truly at risk of losing access to password-protected content if a smartphone locks without the police having connected it to a trusted source or obtained the password voluntarily from the owner.[8] But whatever the answer to that question,

---

[8] Law enforcement under these circumstances might be able to obtain access to password-protected content in a number of ways. First, the police might be able to require arrestees to turn over their passwords; the United States has argued in the lower courts that an individual lacks any Fifth Amendment right to withhold (or refuse to disable) a password, and some courts have accepted this argument. *See, e.g.*, *United States v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009); *United States v.*

there can be no doubt that the State's speculations fail to establish any categorical need to search *all* smartphones – no matter the circumstances under which they are seized or how long after the seizure they are examined – without a warrant.

3. Identification

Lastly, the State suggests that officers need to search smartphones to identify arrestees. Resp. Br. 31. But the interest in identification relates only to the administrative processing of arrestees. *See King*, 133 S. Ct. at 1971, 1974. This Court has never recognized identification as an independent basis for *searches incident to arrest*. Indeed, when arrestees are apprehended inside their homes, there are no doubt numerous effects close at hand that could identify them – letters, certificates, and personal

---

Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); *contra In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012). If the United States is correct, then law enforcement seemingly has nothing to fear regarding passwords. Second, "some protection mechanisms can be bypassed" in police forensic labs. Resp. Br. 35; *accord* Br. of Ass'n of State Crim. Investigative Agencies et al. 10, 15. Third, cell phone manufacturers appear willing to unlock phones the police are unable to unlock themselves. *See* Cal. Dist. Att'ys Ass'n, Cell Phone Records Training Materials 3753-54, https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_irvine1_irvineca.pdf (providing exemplars for orders to Apple and Google to assist in searching phones by "bypassing the Cell Phone user's passcode"); Declan McCullagh, *How Apple and Google Help Police Bypass iPhone, Android Lock Screens*, CNet (April 2, 2012), http://www.cnet.com/news/how-apple-and-google-help-police-bypass-iphone-android-lock-screens/.

documents – but the Court has never excepted these items from *Chimel*'s limitations on searches.

At any rate, there are far more direct, accurate, and less intrusive methods of identifying arrestees, including looking inside their wallets – not to mention fingerprinting and DNA. *See King*, 133 S. Ct. at 1977.

C. None Of The State's Or The United States' Attempts To Mitigate The Implications Of Their Positions Is Persuasive.

Perhaps recognizing the startling implications of the categorical rule they seek, the State and United States offer various proposals for limiting the impact of a decision in their favor. None succeeds.

1. Contrary to the State's suggestions (Resp. Br. 52-57), this Court cannot simply leave it to others to restrict the scope of smartphone searches. This Court, not legislatures, determines the Fourth Amendment's meaning. In any event, legislatures show no sign of entering this realm. Nor can protecting smartphone privacy be left to officer discretion. The Bill of Rights "protects against the Government; it does not leave us at the mercy of *noblesse oblige*." *United States v. Stevens*, 130 S. Ct. 1557, 1591 (2010). Accordingly, this Court will not uphold an otherwise unconstitutional power "merely because the Government promise[s] to use it responsibly." *Id.*[9]

---

[9] The United States asserts that requiring a warrant would not constrain officer discretion because warrants would merely

Nor can this Court leave problems of scope to future cases. The State urges this Court to hold that examining the photo and video files on petitioner's phone was reasonable because at least those particular digital files "are not fundamentally different from, or more sensitive than, other types of personal information long carried by individuals in non-digital forms." Resp. Br. 43. But this argument ignores the sheer quantities of information that smartphones enable people to carry. *See* Petr. Br. 26-27; Br. of CDT & EFF 7-8. No one can lug around thousands of non-digital photos or videos. Nor would anyone have any customary reason even to try to do so. The pervasiveness of smartphone technology, by contrast, practically requires people to bring such information along with them wherever they go.

Adopting the State's reasoning would also be tantamount to holding that police officers can search virtually any file on a smartphone. Certainly emails are no more "fundamentally different from" non-digital information than digital photos and videos are. Nor are personal letters or business documents kept on smartphones (or iPads or laptops) fundamentally different from non-digital papers.

---

specify that "the 'place' to be searched is the cell phone." U.S. Br. 24. But there is no reason why the Fourth Amendment's particularity requirement should dissipate in the digital sphere. Nor have magistrates thought so. *See, e.g.*, Search and Seizure Warrant, *In re Search of an Apple I-Phone Model A1332*, No. 1:12-mj-304 (W.D. Mich. Oct. 9, 2012) (identifying specific areas to be searched, including "historical information regarding call activity, 'phone book' directory information, stored voice-mails and text messages").

Even medical and banking records have long existed in tangible form and occasionally been carried by individuals.

To the extent the State's proposed formula has any capacity to limit searches of smartphones, it is anyone's guess how the formula would apply to numerous types of information commonly found on such devices. Does the Facebook app contain fundamentally different information from the non-digital world? How about an online dating app? Or Confession, an app supported by the Vatican that allows Catholics to record sins and examine their conscience?[10] Police officers and others involved in the criminal justice system need these answers now, not years into the future through endless app-by-app litigation.

2. The United States tenders three different limitations of its own, but none works.

a. Contrary to the United States' contentions (Br. 28-30), a rule limiting smartphone searches to situations when "officers reasonably believe that a phone contains evidence of the offense of arrest" would lack any basis in precedent and, at any rate, would not meaningfully curtail searches. As Justice Scalia explained in *Thornton*, the "reasonable belief" exception is "limited, of course, to searches of motor vehicles, a category of 'effects' which give rise to a reduced expectation of privacy." 541 U.S. at 631 (opinion concurring in judgment). Private papers on smartphones, by contrast, are people's "dearest

---

[10] *Catholic Church Gives Blessing to iPhone App*, BBC (Feb. 8, 2011), http://www.bbc.com/news/technology-12391129.

property," *Entick v. Carrington*, (1765) 95 Eng. Rep. 807, 817-18 (K.B.) – information that is subject to *enhanced* expectations of privacy. It is therefore unsurprising that no historical authority allows exploratory searches of such material for mere evidence of crime. *See Thornton*, 541 U.S. at 631 (Scalia, J., concurring in judgment); Petr. Br. 32, 34-36.

Applying a reasonable-belief test to smartphones would also swallow a general rule prohibiting warrantless searches. The United States asserts that "most traffic offenses" and other minor offenses "would not justify a search of an arrestee's cell phone under [the reasonable-belief] standard." Resp. Br. 29. But the Government ignores that smartphones contain information relevant to the most typical of all traffic offenses: speeding. Petr. Br. 41; *see also Jones*, 132 S. Ct. at 963 (Alito, J., concurring in judgment) (phone GPS tracks a user's "speed of movement"); Sahas Katta, *How My Smartphone Got Me Out of a Speeding Ticket in Traffic Court*, Skatter Tech (Feb. 21, 2011) (describing case in which such evidence was used).[11] The United States also contends that a hunch that a person arrested for possessing firearms might have photos relevant to that charge satisfies the reasonable-belief test. U.S. Br. 30-31. If so, then surely a hunch that a person arrested for DUI (the most common misdemeanor for which people are arrested, *see* Petr. Br. 2 n.2) might

---

[11] http://skatter.com/2011/02/how-my-smart-phone-got-me-out-of-a-speeding-ticket-in-traffic-court/.

have relevant photos from earlier that evening would satisfy that test as well. One could go on and on.

The only logical inference, therefore, to be drawn from the United States' comments respecting traffic and other minor offenses is that even the Government senses how outrageous it would be to search people's smartphones incident to arrest for such offenses. But any such carve-out would run headlong into this Court's precedent. As this Court explained in *Robinson*, at the behest of the United States itself, "all custodial arrests" – no matter how petty the offense – must be "treat[ed] . . . alike for purposes of [the search incident to arrest doctrine]." 414 U.S. at 235.

b. Although Arizona and other states urge this Court to eschew any holding that "would require officers to make impromptu decisions regarding the appropriateness of a particular search based upon a myriad of factors associated with each particular arrest," Br. 2-3, the United States next suggests that officers should be permitted to search "the areas of the phone reasonably related to finding evidence relevant to the crime of arrest, identifying the arrestee, and protecting officers." U.S. Br. 30. Such an "area by area" approach would generate an administrative nightmare. Data on smartphones is increasingly interwoven and impossible to separate. A "contacts" file, for example, typically culls and integrates data from the phone's social networking apps; a calendar can sync with GPS-tracking software; and "text" messages now include private photos, videos, business and medical notifications, and more. How would an officer decide which of a phone's various apps with overlapping information

would be appropriate to search? How far back in time within each app can a search go? Can links to external information found during these searches be activated? The United States provides no answers.

c. Lastly, referencing *Chimel*'s "spatial limit" on searches incident to arrest, the United States argues that remotely stored data, as opposed to data saved on a phone, is physically outside the arrestee's "reaching distance" and thus off-limits. U.S. *Wurie* Br. 43-44. But this analogy to an arrestee's physical environment is nonsense. That digital information is stored remotely does not make it any less accessible to the holder of a phone.

In any event, precluding officers from "affirmatively us[ing]," U.S. Br. 34, smartphones to examine digital material stored elsewhere would not meaningfully curtail the scope of smartphone searches. Smartphones continually pull down new data on their own from remote servers. Smartphones also are designed so that "the data that is stored on the phone and the data that is stored in the cloud and available on the phone are often indistinguishable." Br. of EPIC 13; *see also* Apple, iOS Human Interface Guidelines 102 (2014) ("Ideally, users don't need to know where their content is located and they should seldom have to think about which version of the content they're currently viewing."). So unless police officers permanently disconnect the phone from its network before conducting any search, they will have no way of knowing whether data displayed on a phone is stored locally or remotely.

Even after a phone has been disconnected from its network, information on apps that comes from remote sources will still usually be on the phone.

Whenever such an app has been launched, it "store[s] at least temporary copies of the accessed material on the phone itself." Resp. Br. 55. Thus, even under the United States' remote-storage restriction, individuals' business, medical, banking, and other highly sensitive information would still be exposed to warrantless exploratory searches.

II. The Search Of Petitioner's Phone At The Stationhouse Was Too Remote From His Arrest To Qualify As A Search Incident To Arrest.

Neither of the State's arguments in defense of the remoteness of the stationhouse search of petitioner's smartphone withstands scrutiny.

A. At least insofar as the stationhouse search of petitioner's smartphone occurred far away from "the *immediate* vicinity of the arrest," *Shipley v. California*, 395 U.S. 818, 819-20 (1969) (per curiam) (quoting *Stoner v. California*, 376 U.S. 483, 486 (1964)), the State does not dispute that the search contravened the remoteness limitation enunciated in this Court's cases. *See* Petr. Br. 44-47 (discussing these cases). But, relying on *Edwards*, the State argues that this remoteness limitation does not apply to items seized at the scene from arrestees. Resp. Br. 25-28.

As petitioner has explained, the dispositive inquiry under *Edwards* is not whether the item was on the arrestee's person when arrested, but instead whether the item was still in his possession "at the place of detention" – and thus still subject to *Chimel*'s

justifications – when seized and inspected. *Edwards*, 415 U.S. at 807; *see* Petr. Br. 48-51.[12] Any other distinction would be completely arbitrary. Whatever reason may exist, with respect to searches in the field, for distinguishing between items seized from persons and their grab areas, there is no difference, with respect to searches at the stationhouse, between an item that was taken two hours ago from an arrestee's pocket and one that was in a piece of luggage or sitting beside him. Petr. Br. 51.

The State responds that "it is hard to see the benefit . . . of insisting that every aspect of the search take place at once, or at the initial scene." Resp. Br. 26. But just as with the automobile searches at issue in *Thornton* and *Gant*, this argument mistakenly "assumes that, one way or another, the [warrantless] search must take place." *Thornton*, 541 U.S. at 627 (Scalia, J., concurring in judgment). Where "sensible police procedures," *id.*, dictate doing the search later at the police station, there is no reason not to apply the traditional warrant requirement. And in this context, good police work nearly always dictates that searches deep into smartphones take place at the station. *See* Br. of Crim. Law Profs. 10-11; NIST Draft Guidelines 37 (flowchart repeatedly instructing police to wait to search devices).

---

[12] The United States notes that the clothing in *Edwards* was "later subjected to laboratory analysis." U.S. Br. 32. The defendant did not challenge that action, which in any event would not have raised privacy concerns anywhere near the ones at issue here.

B. It makes no difference that petitioner's smartphone was "first examined at the original scene." Resp. Br. 26. This Court has never adopted the "second look" doctrine on which the State relies. Nor should it. That police have grounds at one moment to conduct a warrantless search does not obviate the need for a warrant in perpetuity. A non-digital analogy is instructive: When the police arrest someone in his home, they may search the area within the arrestee's reach and conduct a protective sweep. But they may not return two days later for a second warrantless search. *See Mincey v. Arizona*, 437 U.S. 385 (1978).

At any rate, whatever the law may be when the police reexamine information that was "fully exposed" to them at the original scene, *United States v. Burnette*, 698 F.2d 1038, 1049 (9th Cir. 1983), an initial cursory glance at a few texts on a smartphone cannot possibly justify a later search of other files on the phone. In such an instance, the later search is really the *first* look, not the second.

CONCLUSION

For the foregoing reasons, the judgment of the California Court of Appeal should be reversed.

Respectfully submitted,

Patrick Morgan Ford
LAW OFFICE OF PATRICK MORGAN FORD
1901 First Avenue
Suite 400
San Diego, CA 92101

Donald B. Ayer
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001

Jeffrey L. Fisher
Counsel of Record
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

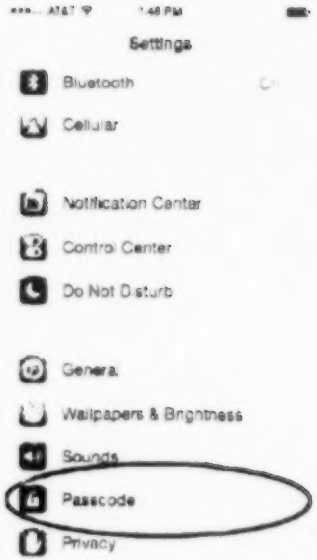
April 22, 2014

APPENDIX

Appendix A

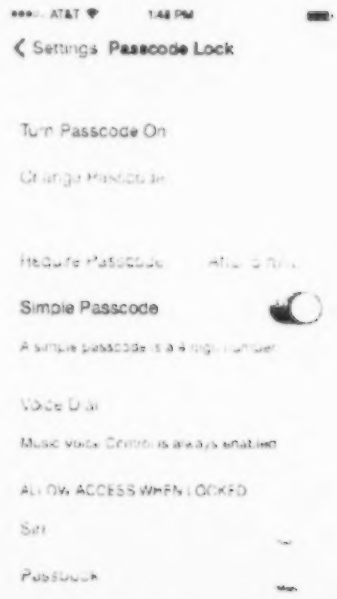
The two steps necessary to put an iPhone in airplane mode, regardless of whether it is locked.

Appendix B



Password enabled

Password disabled



The two steps necessary to determine whether an iPhone has password-protection.

Appendix C

The four steps necessary to disable the auto-lock feature through an iPhone's settings.

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
APR - 9 2014
OFFICE OF THE CLERK

No. 13-132

In the Supreme Court of the United States

DAVID LEON RILEY, PETITIONER

v.

STATE OF CALIFORNIA

ON WRIT OF CERTIORARI
TO THE COURT OF APPEAL OF CALIFORNIA,
FOURTH APPELLATE DISTRICT, DIVISION ONE

BRIEF FOR THE UNITED STATES AS AMICUS CURIAE SUPPORTING RESPONDENT

DONALD B. VERRILLI, JR.
Solicitor General
Counsel of Record
DAVID A. O'NEIL
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
JOHN F. BASH
Assistant to the Solicitor General
ROBERT A. PARKER
Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

Library of Congress
Law Library

QUESTION PRESENTED

Whether evidence admitted at petitioner's trial was obtained in a search of petitioner's cell phone that violated petitioner's Fourth Amendment rights.

TABLE OF CONTENTS

Page

Interest of the United States 1
Statement 1
Summary of argument 4
Argument:
I. The Fourth Amendment permitted officers to search petitioner's cell phone incident to his arrest 7
A. *Chimel* does not support precluding the police from searching a cell phone incident to arrest 8
B. Privacy concerns do not justify a cell-phone exception to officers' search-incident-to-arrest authority 21
C. A total prohibition on cell-phone searches incident to arrest cannot be justified 28
D. The search of petitioner's cell phone was lawful 30
II. The stationhouse search of petitioner's cell phone occurred within a reasonable time after his arrest 31
Conclusion 35
Appendix 1a

TABLE OF AUTHORITIES

Cases:

A Quantity of Copies of Books v. *Kansas*, 378 U.S. 205 (1964) 26
Andresen v. *Maryland*, 427 U.S. 463 (1976) 24
Arizona v. *Gant*, 556 U.S. 332 (2009) 10, 28
Chimel v. *California*, 395 U.S. 752 (1969) 4, 8
City of Ontario, Cal. v. *Quon*, 130 S. Ct. 2619 (2010) 21, 34
Cooper v. *California*, 386 U.S. 58 (1967) 32

Cases—Continued: Page

Dillon v. *O'Brien & Davis*, 16 Cox C.C. 245 (Exch. Div. Ir. 1887) 22
Dyke v. *Taylor Implement Mfg. Co.*, 391 U.S. 216 (1968) 33
Fernandez v. *California*, 134 S. Ct. 1126 (2014) 20
Florence v. *Board of Chosen Freeholders*, 132 S. Ct. 1510 (2012) 31, 35
Gouled v. *United States*, 255 U.S. 298 (1921), overruled on other grounds by *Warden* v. *Hayden*, 387 U.S. 294 (1967) 25
Hill v. *California*, 401 U.S. 797 (1971) 25
Kentucky v. *King*, 131 S. Ct. 1849 (2011) 20
Kyllo v. *United States*, 533 U.S. 27 (2001) 8
Marcus v. *Search Warrant*, 367 U.S. 717 (1961) 26, 27
Maryland v. *King*, 133 S. Ct. 1958 (2013) 9, 10
Missouri v. *McNeely*, 133 S. Ct. 1552 (2013) 9, 13
NAACP v. *Alabama ex rel. Patterson*, 357 U.S. 449 (1958) 28
People v. *Diaz*, 244 P.3d 501, cert. denied, 132 S. Ct. 94 (2011) 4
Preston v. *United States*, 376 U.S. 364 (1964) 33
Roaden v. *Kentucky*, 413 U.S. 496 (1973) 26, 27
Stanford v. *Texas*, 379 U.S. 476 (1965) 6, 27
Steagald v. *United States*, 451 U.S. 204 (1981) 23
Terry v. *Ohio*, 392 U.S. 1 (1968) 29
Thornton v. *United States*, 541 U.S. 615 (2004) 10, 28, 29
United States v. *Bennett*, 409 F.2d 888 (2d Cir.), cert. denied, 396 U.S. 852 (1969) 26
United States v. *Chadwick*, 433 U.S. 1 (1977), abrogated by *California* v. *Acevedo*, 500 U.S. 565 (1991) 8, 10, 28, 32

Cases—Continued: Page

United States v. *Edwards*, 415 U.S. 800 (1974) ..... *passim*
United States v. *Flores-Lopez*, 670 F.3d 803 (7th Cir. 2012) 14
United States v. *Kirschenblatt*, 16 F.2d 202 (2d Cir. 1926) 6, 26
United States v. *Lefkowitz*, 285 U.S. 452 (1932) 26
United States v. *Robinson*, 414 U.S. 218 (1973) ..... *passim*
United States v. *$639,558 in U.S. Currency*, 955 F.2d 712 (D.C. Cir. 1992) 33
United States v. *Smith*, 565 F.2d 292 (4th Cir. 1977) 22
United States v. *Steiger*, 318 F.3d 1039 (11th Cir.), cert. denied, 538 U.S. 1051 (2003) 34
United States v. *Williams*, 592 F.3d 511 (4th Cir.), cert. denied, 131 S. Ct. 595 (2010) 24
Warden v. *Hayden*, 387 U.S. 284 (1967) 22
Weeks v. *United States*, 232 U.S. 383 (1914) 7, 33
Wilkes v. *Wood*, 98 K.B. 489 (1763) 23
Zurcher v. *Stanford Daily*, 436 U.S. 547 (1978) 25

Constitution and statutes:

U.S. Const.:
Amend. I 25, 26
Amend. IV ..... *passim*
Omnibus Crime Control and Safe Streets Act of 1968, Tit. III, 18 U.S.C. 2511-2522 34
Stored Communications Act, 18 U.S.C. 2701 34
18 U.S.C. 2703(a) 34
Cal. Penal Code (West 2008):
§ 187(a) 3
§ 245(b) 3
§ 246 3

Statutes—Continued: Page

§ 664 3
§ 12025(a)(1) 2
§ 12025(b)(3) 30
§ 12031(a)(1) 2
§ 12031(a)(1)(C) 30

Miscellaneous:

Apple, Inc.:
iOS Security (Oct. 2012), https://www.apple.com/ipad/business/docs/iOS_Security_Oct12.pdf 11, 12, 13
iPhone User Guide for iOS 7.1 (Mar. 2014), http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf 11
Rick Ayers et al., National Institute of Standards and Technology, U.S. Department of Commerce, *Guidelines on Mobile Device Forensics (Draft)* (Sept. 2013), www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf 12, 13, 14, 15, 16, 18
David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, Forensic Focus (Aug. 20, 2011), http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations 15, 18
Bureau of Justice Statistics:
Federal Law Enforcement Officers, www.bjs.gov/index.cfm?ty=pbdetail&iid=4372 (last visited Apr. 9, 2014) 17

Miscellaneous—Continued: Page

Local Police, www.bjs.gov/index.cfm?ty=tp&tid=71 (last visited Apr. 9, 2014) 17

Eoghan Casey & Benjamin Turnbull, *Digital Evidence on Mobile Devices*, reprinted in *Digital Evidence and Computer Crime* (3d ed. 2011), http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf 13, 15, 16, 18, 19

Digital Shield, Inc., *Cellebrite UFED Certified Training*, www.digitalshield.net/cellebriteinfo.php 17

Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49 (2013) 23

Ronen Engler & Christa M. Miller, *6 Persistent Challenges with Smartphone Forensics*, Digital Forensic Investigator News (Feb. 8, 2013), www.dfinews.com/articles/2013/02/6-persistent-challenges-smartphone-forensics 18

FBI, *Mobile Forensics Field Guide: What Every Peace Officer Must Know*, V.2.0 (2010) 13, 15, 19

Simson Garfinkel, *The iPhone Has Passed a Key Security Threshold*, MIT Technology Review (Aug. 13, 2012), www.technologyreview.com/news/428477/the-iphone-has-passed-a-key-security-threshold 11, 12

Greg Gogolin, *Digital Forensics Explained* (2013) 15, 17, 18, 19

http://docs.blackberry.com/en/admin/deliverables/16648/Encrypting_user_data_on_a_locked_BB_device_834471_11.jsp (last visited Apr. 9, 2014) 12

http://source.android.com/devices/tech/security (last visited Apr. 9, 2014) 12

Miscellaneous—Continued: Page

Eric Katz, *A Field Test of Mobile Phone Shielding Devices* (Dec. 10, 2010) (published M.S. thesis, Purdue University), http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters 16

Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, 33 Conn. L. Rev. 503 (Winter 2001) 12

Richard P. Mislan et al., *The Growing Need for On-Scene Triage of Mobile Devices*, 6 Digital Investigation 112 (2010) 14, 15, 19

Press Release, U.S. Attorney's Office, S.D. Ga., Martinez Man Sentenced to More Than 24 Years for Attempted Online Enticement of a Minor and Destruction of Evidence (Jan. 22, 2014), www.fbi.gov/atlanta/press-releases/2014/ martinez-man-sentenced-to-more-than-24-years-for-attempted-online-enticement-of-a-minor-and-destruction-of-evidence 19

Product Information: Cellebrite UFED Touch Ultimate, SC Mag. (May 1, 2013), www.scmagazine.com/cellebrite-ufed-touch-ultimate/review/3870 ..... 17, 19

Samsung Instinct User Guide (2008), http://support.sprint.com/global/pdf/user_guides/samsung/instinct/samsung_instinct_ug.pdf 14

In the Supreme Court of the United States

No. 13-132

DAVID LEON RILEY, PETITIONER

v.

STATE OF CALIFORNIA

ON WRIT OF CERTIORARI
TO THE COURT OF APPEAL OF CALIFORNIA,
FOURTH APPELLATE DISTRICT, DIVISION ONE

BRIEF FOR THE UNITED STATES AS AMICUS CURIAE SUPPORTING RESPONDENT

INTEREST OF THE UNITED STATES

This case involves the Fourth Amendment implications of a police search of the contents of a cell phone found on a person after his lawful custodial arrest. Federal prosecutors rely on such evidence in federal criminal cases, and federal law-enforcement officers conduct similar cell-phone searches. This Court has granted certiorari in *United States* v. *Wurie*, No. 13-212, to consider related issues.

STATEMENT

1. A San Diego police officer stopped a vehicle driven by petitioner after noticing that it had expired tags. Pet. App. 3a, 5a. During the stop, the officer learned that petitioner had a suspended license. *Id.* at 5a. Consistent with departmental policy, the officer decided to impound the vehicle. *Ibid.* An inventory

search of the car at the scene revealed two handguns under its hood. *Id.* at 3a, 5a-6a. The officer then arrested petitioner for possession of concealed firearms. *Id.* at 6a; J.A. 23; see Cal. Penal Code §§ 12025(a)(1), 12031(a)(1) (West 2008).

The officer searched petitioner's person incident to the arrest, finding paraphernalia associated with the Lincoln Park Bloods, a violent street gang, and a cell phone. J.A. 8. The officer examined petitioner's cell phone and noticed that in certain textual entries, every word that began with the letter "K" was preceded by a "C." *Ibid.* He recognized that misspelling to be an abbreviation for "Crip Killer," indicating that petitioner was a member of the rival Bloods. *Ibid.*

The arresting officer contacted a detective specializing in gangs. About two hours later, at the stationhouse, the detective interviewed petitioner, whom he recognized as a member of the Lincoln Park gang and whom he suspected of involvement in a shooting three weeks earlier. J.A. 15-17; see Br. in Opp. 2. Because the detective knew that "gang members will often video themselves with guns or take pictures of themselves with the guns," he examined the contents of petitioner's phone to obtain "further evidence to prove that he was in possession of th[e] firearms that the officers found inside the car." J.A. 20; see Pet. App. 6a-7a. Some of the video clips on the phone depicted street boxing, a common gang-initiation activity. J.A. 11-12. Petitioner was heard on one clip shouting words of encouragement and referring to one of the boxers as "Blood." J.A. 12-13. The detective also observed photos of petitioner making gang signs. J.A. 30-32, 42-44.

2. a. In connection with the earlier shooting, petitioner was charged in the Superior Court of California with one count of attempted murder, Cal. Penal Code §§ 187(a), 664 (West 2008), one count of shooting at an occupied vehicle, *id.* § 246, and one count of assault with a semiautomatic firearm, *id.* § 245(b). Pet. App. 1a. He moved to suppress the videos and photographs showing his gang affiliation obtained from the search of his cell phone. *Id.* at 4a.

The superior court denied petitioner's suppression motion. J.A. 21-24. The court explained that under the search-incident-to-arrest doctrine articulated in *United States* v. *Robinson*, 414 U.S. 218 (1973), and *United States* v. *Edwards*, 415 U.S. 800 (1974), "in the case of a lawful arrest, a full search of the person is an exception to the warrant requirement of the [F]ourth [A]mendment and is reasonable under that amendment." J.A. 23. Applying that principle, the court further explained, courts "have allowed items on the person to be searched, including wallets, address books, papers and the like." *Ibid.* "Cell phones do contain personal information," the court noted, "but really no more so than wallets and purses and address books." *Ibid.* Because petitioner's cell phone "was on his person at the time of arrest," the court held, it "was taken out of the realm [of] protection [from] police interest for a reasonable time following the arrest." *Ibid.* The court also found that the search was part of "an investigation relating to the crime for which [petitioner] was arrested, which was the finding of the guns in the car." *Ibid.*

b. After a hung jury in petitioner's first trial, he was retried, and the superior court again ruled the phone evidence admissible. J.A. 26. At the second

trial, officers testified about the photos and videos on petitioner's phone, and three of the photos were admitted. J.A. 30-44. Petitioner was convicted on all counts and sentenced to a term of imprisonment of 15 years to life. Pet. App. 1a. Petitioner separately pleaded guilty to offenses arising out of the traffic stop, including carrying a concealed firearm in a vehicle. Pet. Br. 7 n.5.

3. The California Court of Appeal affirmed. Pet. App. 1a-23a. Relying on the California Supreme Court's decision in *People* v. *Diaz*, 244 P.3d 501, cert. denied, 132 S. Ct. 94 (2011), the court held that because petitioner's "cell phone was immediately associated with his person when he was arrested," the search of the phone "was lawful whether or not an exigency * * * existed." Pet. App. 15a (internal quotation marks omitted).

SUMMARY OF ARGUMENT

I. The Fourth Amendment permitted officers to search petitioner's cell phone incident to his lawful arrest. This Court has long confirmed that officers possess "unqualified authority" to search the person of an arrestee and any objects or containers found on his person for evidence of crime. *United States* v. *Robinson*, 414 U.S. 218, 225 (1973). Petitioner has not identified a single decision of this Court or any historical or practical basis supporting an item-specific exception to that rule.

A. Contrary to petitioner's view, the narrowly focused law-enforcement interests set forth in *Chimel* v. *California*, 395 U.S. 752 (1969), do not support excluding cell phones from officers' search authority. Those interests have never delimited officers' authority to search objects on the person—an authority that rests

primarily on the reduced expectation of privacy caused by a lawful arrest, as well as the police's overriding interest in gathering evidence of crime during the critical period immediately following an arrest in a place where it is particularly likely to be found.

In any event, cell phones implicate the *Chimel* justifications more powerfully than virtually any other object. Unlike the physical contents of a container, digital contents can be concealed or destroyed before a warrant can be obtained even once the container is in police custody—sometimes within minutes. When an officer finds an unlocked cell phone at the scene of an arrest, searching it immediately may be her only chance to retrieve and preserve essential evidence. Petitioner's proposed solutions to that serious problem—such as equipping every officer with unwieldy forensic devices that cost several thousand dollars each—are entirely unrealistic.

B. Cell phones do not raise qualitatively different privacy concerns than items that the police have always had authority to search incident to arrest, such as letters, diaries, briefcases, and purses. Evidence of crime should not be insulated from traditional review because the arrestee maintains it in a technologically sophisticated form. Cell phones may contain a significantly greater quantity of information than traditional items, but where, as here, the search is conducted before "the administrative mechanics of arrest have been completed and the prisoner is incarcerated," *United States* v. *Edwards*, 415 U.S. 800, 804 (1974), officers would not be able to peruse the entire contents of the arrestee's cell phone.

Petitioner contends that cell phones' capacity to contain expressive material, such as text messages

and photos, calls for a special restriction on the police's search authority. But "the law has never distinguished between documents and other property found upon the person of one arrested." *United States* v. *Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.). The precedents petitioner cites concern either pre-*Chimel* searches of the *premises* of arrest, or seizures of expressive materials where "the basis for their seizure [was] the ideas which they contain[ed]," *Stanford* v. *Texas*, 379 U.S. 476, 485 (1965). They have no application here, and *Robinson* states the controlling test.

C. If the Court were inclined to resolve this case on narrower grounds, the government suggested two alternative approaches in its opening brief in *United States* v. *Wurie*, No. 13-212. One approach would permit officers to search a phone incident to arrest only when it is reasonable to believe that it contains evidence relevant to the offense of arrest; a second would limit the *scope* of any cell-phone search incident to arrest to actions reasonably related to legitimate law-enforcement objectives. U.S. *Wurie* Br. 45-55. Petitioner addresses only the first approach, contending that it would impose no meaningful limitation (while paradoxically maintaining that it would invalidate the search in this case). But an offense-of-arrest approach would prevent officers from searching cell phones incident to arrest for traffic offenses and other minor crimes where evidence could not be reasonably expected to be found on the phone.

D. Whether the Court applies *Robinson* or either of the narrower approaches the United States articulated, the search in this case was lawful: the cell phone was found on petitioner's person; the officers

had reason to believe it contained evidence of crime; and the search sought such evidence.

II. Petitioner's objection to the stationhouse search of his phone about two hours after his arrest lacks merit. This Court approved a delay of ten hours in *Edwards*. Here, the delay was much less and, as in *Edwards*, the search occurred before the administrative mechanics of arrest were completed. Deferring the search was particularly reasonable given that the on-the-scene search indicated that petitioner was likely involved in gang activity, and the arresting officer appropriately contacted a detective with special expertise in gangs, who examined the phone once it was brought to the stationhouse.

ARGUMENT

I. THE FOURTH AMENDMENT PERMITTED OFFICERS TO SEARCH PETITIONER'S CELL PHONE INCIDENT TO HIS ARREST

As the United States explained in its opening brief in *United States* v. *Wurie*, No. 13-212, this Court has long confirmed that the police may "search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime," without obtaining a warrant, and that this procedure includes examining any object found on the person. *United States* v. *Robinson*, 414 U.S. 218, 224-225 (1973) (quoting *Weeks* v. *United States*, 232 U.S. 383, 392 (1914)).

In arguing that the police lacked authority to search his cell phone after he was arrested for concealing firearms under the hood of his car, petitioner contends, as did the First Circuit in *Wurie*, first, that the search of a cell phone does not advance the interests that this Court has invoked in defining the permissible spatial extent of a search of the *premises* of

arrest under *Chimel* v. *California*, 395 U.S. 752 (1969); and, second, that cell phones raise different privacy concerns than other objects, in part because they contain written material and other media.

Those arguments should be rejected. Far from preserving "that degree of privacy against government that existed when the Fourth Amendment was adopted," *Kyllo* v. *United States*, 533 U.S. 27, 34 (2001), petitioner's view would give arrestees a right that they have never had: protection against a full search of their persons and the effects found on their persons incident to a probable-cause arrest.

A. *Chimel* Does Not Support Precluding The Police From Searching A Cell Phone Incident To Arrest

Petitioner contends (Br. 15-24) that permitting the police to search a cell phone found on the person of an arrestee would "sever the search-incident-to-arrest doctrine forevermore from its conceptual underpinnings" (Br. 18) by allowing searches that do not serve the particularized interests identified in *Chimel*. That argument is wrong both legally and factually.

1. As the United States explained in *Wurie* (Br. 13-28), this Court's decisions have never held that the full authority to search the person of an arrestee, including any item found on his person, is limited by the particularized justifications—officer safety and the preservation of evidence that might be concealed or destroyed—set forth in *Chimel*. To the contrary, it has explained that the authority to search the person of an arrestee is primarily "justified by [the] reduced expectations of privacy caused by the arrest." *United States* v. *Chadwick*, 433 U.S. 1, 16 n.10 (1977), abrogated on other grounds by *California* v. *Acevedo*, 500 U.S. 565 (1991). Last Term, the Court twice reiterat-

ed that an arrest categorically authorizes the full search of the person of the arrestee. See *Maryland* v. *King*, 133 S. Ct. 1958, 1970-1971 (2013); *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1559 n.3 (2013).

Petitioner nevertheless contends that the *Chimel* justifications narrow not only the spatial breadth of the search area around an arrestee, but also the types of items found on the person of an arrestee that the police may search. *Robinson*, *supra*, rejected precisely that argument. See 414 U.S. at 235. Petitioner would recast *Robinson* as resting exclusively on the need for officers to make "quick ad hoc judgment[s]" in arrest situations, *ibid.*, an interest he believes is not advanced by searches of digital contents. Pet. Br. 18. That is wrong. Although *Robinson* described that important interest as a benefit of the traditional rule, its holding is that if an arrest is lawful, a search of the person of the arrestee "requires no additional justification." 414 U.S. at 235.

Under petitioner's reasoning, *Robinson*—as well as this Court's post-*Robinson* cases applying the same principle—were all wrongly decided. Petitioner's central premise is that "[o]nce the police have exclusive control over a smart phone and have secured it beyond an arrestee's grab area, there is no legitimate concern that the arrestee could alter or destroy the phone's digital contents." Pet. Br. 21. But precisely the same thing could have been said of the cigarette package at issue in *Robinson*—or any other object or container. Petitioner's only attempt to reconcile *Robinson*'s holding with his reasoning is to observe in a footnote that the police in the 1970s often gave cigarette packages back to arrestees. *Id.* at 19 n.7. The Court's opinion made no mention of that purported practice. In any

event, petitioner surely would not concede that a cell-phone search becomes lawful if the officer returns the phone after examining its contents.

Petitioner also contends that this Court's post-*Robinson* decisions in *Chadwick*, *supra*, and *Arizona* v. *Gant*, 556 U.S. 332 (2009), support his view. But as the United States explained in *Wurie* (Br. 21-23), both of those cases concerned the area around the arrestee, for which he has no reduced expectation of privacy, and neither decision cast doubt on officers' longstanding categorical authority to search items found on the *person* of an arrestee.

Furthermore, as Justice Scalia explained in *Thornton* v. *United States*, 541 U.S. 615 (2004), the search-incident-to-arrest doctrine was traditionally grounded in the "interest in gathering evidence relevant to the crime for which the suspect had been arrested." *Id.* at 629 (concurring in the judgment); see U.S. *Wurie* Br. 15. Searches of the arrestee's person were also justified based on officers' time-sensitive need to ascertain or confirm a suspect's identity. See *ibid.*; see also *King*, 133 S. Ct. at 1971. Petitioner does not argue that cell-phone searches fail to advance those historical justifications.

2. Not only is petitioner incorrect that cell-phone searches incident to arrest are justifiable only if officers "need to search [their] data to protect against the destruction of evidence" or ensure officer safety, Pet. Br. 16, he also misunderstands the tremendous challenges that mobile-communication technology poses in arrest situations. In light of those challenges it will often be critical that officers search a suspect's cell phone as soon as practicable after an arrest is made.

a. When an arresting officer finds an unlocked cell phone that may contain evidence of crime, she has sound reason to examine its contents immediately. See U.S. *Wurie* Br. 34-37. Most modern cell phones can be programmed to lock automatically after some period of inactivity—for example, between one minute and four hours on Apple's iPhone. See *iPhone User Guide for iOS 7.1*, at 10 (Mar. 2014) (iPhone Manual).[1] Once locked, data on the phone will be protected by sophisticated encryption walls that make it very difficult, and often impossible, to recover any information from the device unless the officers acquire the arrestee's passcode.

The iPhone, for example, uses an "AES [Advanced Encryption Standard] 256-bit key[] fused into the application processor during manufacturing." Apple, Inc., *iOS Security* 7 (Oct. 2012) (*iOS Security*).[2] In practice, that means that once locked, the iPhone is essentially "unbreakable": "no computer imaginable for the foreseeable future * * * would be able to crack a truly random 256-bit AES key." Simson Garfinkel, *The iPhone Has Passed a Key Security Threshold*, MIT Technology Review (Aug. 13, 2012).[3] Other device manufacturers and operating systems use similar methods to protect user data. Even for phones that use less sophisticated encryption technology than the iPhone, "the decryption of even a short

---

[1] http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

[2] https://www.apple.com/ipad/business/docs/iOS_Security_Oct12.pdf.

[3] www.technologyreview.com/news/428477/the-iphone-has-passed-a-key-security-threshold.

key would consume extraordinary amounts of government resources." Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, 33 Conn. L. Rev. 503, 530 (Winter 2001).[4]

Turning off a phone or removing its battery—steps that petitioner and his amici confidently recommend—only exacerbates that encryption problem. While a cell phone is still powered on, a copy of the encryption key may remain saved in the device's accessible memory, making it possible in some instances for forensic labs, through a painstaking process, to recover the key. But once a phone is turned off, "the copy of the encryption key in the computer's accessible memory is erased," making it far more daunting to decrypt the device. Garfinkel, *supra*; see also Rick Ayers et al., National Institute of Standards and Technology, U.S. Department of Commerce, *Guidelines on Mobile Device Forensics (Draft)* 30-31 (Sept. 2013) (NIST Draft Guidelines).[5]

In addition to attempting to circumvent the encryption wall, law-enforcement agencies can try to ascertain the user's passcode. But it may take years of work in a forensic laboratory to break even a simple passcode. See *iOS Security* 9 (five-and-a-half years for a six-character alphanumeric passcode); Garfinkel, *supra* (25 years for a 10-digit numeric passcode). Re-

---

[4] See, *e.g.*, http://source.android.com/devices/tech/security (Google Android); http://docs.blackberry.com/en/admin/deliverables/16648/Encrypting_user_data_on_a_locked_BB_device_834471_11.jsp (Blackberry).

[5] www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

alistically, law-enforcement agencies will not have the resources to attempt to break a passcode for any but the most serious cases. And even if great resources were applied, many phones have security features that thwart attempts to overcome the passcode. Apple, for example, allows a user "to have the device automatically wiped after 10 failed passcode attempts." *iOS Security* 9.

If ever a circumstance implicated the *Chimel* evidence-preservation interest, therefore, this is it. The combination of automatic locking and encryption means that officers who seize an unlocked cell phone—which may forever conceal its contents within a matter of minutes or hours—will have no idea, until it is too late, whether they can "reasonably obtain a warrant * * * without significantly undermining the efficacy of the search." *McNeely*, 133 S. Ct. at 1561. That is why forensic guides recommended that "[w]here possible, devices supporting encryption, such as Android and [Apple] iOS devices, should be triage processed at the scene if they are found in an unlocked state, as the data may no longer be available to an investigator once the device's screen is locked, or if the battery exhausts." NIST Draft Guidelines 35; accord FBI, *Mobile Forensics Field Guide: What Every Peace Officer Must Know* 3, V. 2.0 (2010) (Mobile Guide) ("Mobile devices can be set to self-lock and/or encrypt after a specified period of time elapses. If the device in question is currently in an unlocked state, but you think it is set to self-lock, immediately examining the device may be the only opportunity to collect evidence."); see Eoghan Casey & Benjamin Turnbull,

Digital Evidence on Mobile Devices 17, reprinted in *Digital Evidence and Computer Crime* (3d ed. 2011);[6] Richard P. Mislan et al., *The Growing Need for On-Scene Triage of Mobile Devices*, 6 Digital Investigation 112, 115 (2010) (Mislan).

b. The threat of "remote wiping" also poses a risk of evidence destruction. See U.S. *Wurie* Br. 37-40. On all major cell-phone platforms, data on a smartphone can quickly be erased by confederates or others who lack physical access to the device. See NIST Draft Guidelines 29; Mislan at 113, 118; *United States* v. *Flores-Lopez*, 670 F.3d 803, 808-809 (7th Cir. 2012). That could be done for at least some information on petitioner's phone. See Samsung Instinct User Guide 76 (2008) (cited Pet. Br. 22) ("If your device is lost or stolen, you can use Sprint Mobile Sync to remotely remove all the contacts information.").[7] And newer "geofencing" technology promises to enable users to preset their phones to automatically erase their contents when brought into a particular location, such as a police station. See U.S. *Wurie* Br. 38-39.

i. Petitioner and his amici suggest a host of solutions to the remote-wiping threat—all of which are far less certain to protect evidence than setting aside a cigarette package or an article of clothing. Petitioner states, for example, that officers could remove the memory card or the battery from the phone. But only some models allow the easy removal of a memory card or the battery, and it may not be obvious from the

---

[6] http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf.

[7] http://support.sprint.com/global/pdf/user_guides/samsung/instinct/samsung_instinct_ug.pdf.

phone's exterior that removal is possible or how to do it. See Casey & Turnbull 17-18. Those steps also risk permanently losing evidence: removing a phone's battery may trigger a password lock that could make any evidence on the phone effectively irretrievable, and removable memory cards are easily damaged and may become encrypted when ejected. *Ibid.*; Mislan at 121.

Petitioner also points (Br. 22-23) to Faraday bags. As the government explained in *Wurie* (U.S. Br. 39-40), those can be effective at blocking a wireless signal, but they have the effect of quickly draining the phone's battery as the phone searches for a wireless signal. NIST Draft Guidelines 30.[8] To function properly, moreover, Faraday bags must be completely sealed—with no holes, gaps, or frays in the material—and even then they may fail to prevent wireless communication if the phone passes near a cell tower, an associated WiFi router, or another place where a signal is particularly strong. *Id.* at 30, 32; Mobile Guide 9 ("Faraday bags are reliable, but can't fully guarantee that signals will not reach the phone. Successfully blocking a signal depends on the quality of the bag, the distance to the closest cell tower, and the power of the transmitter in the mobile device."); David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, Forensic

---

[8] Although battery drain could be averted by connecting the phone to a portable power source placed inside the Faraday bag, that would require every officer to carry a fully charged portable power source at all times, along with power cord adapters compatible with every type of phone. See Greg Gogolin, *Digital Forensics Explained* 59-60 (2013).

Focus (Aug. 20, 2011).[9] A Purdue University study found that, in a majority of cases, Faraday bags and similar enclosures "did not prevent network communication in all cases, and SMS [text] messages most often penetrated the device while shielded, followed by voice calls and MMS [multimedia] messages"—messages that could trigger remote wiping. NIST Draft Guidelines 32; see Eric Katz, *A Field Test of Mobile Phone Shielding Devices* (Dec. 10, 2010) (published M.S. thesis, Purdue University).[10]

Furthermore, because a remote-wiping command will be received and executed as soon as the phone reconnects to a network, the phone must continue to be shielded once it is removed from the bag. NIST Draft Guidelines 33. That means that local police departments will need not only cheap Faraday bags, but also Faraday *rooms* or other specialized equipment enveloped in protective material. *Ibid.*; Casey & Turnbull, 17.

Another option for preventing remote wiping is to put the phone in "airplane mode," which turns off the device's wireless communications. But to accomplish that successfully, an officer must be familiar with the configuration of each device she encounters, which can be challenging given the wide variation among different models of devices and versions of operating systems, as well as the ability of service providers and users to customize the appearance, layout, and default

---

[9] http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations.

[10] http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters.

language of each device. See Greg Gogolin, *Digital Forensics Explained* 57 (2013). And as with Faraday bags, putting a phone in airplane mode does nothing to prevent the phone from locking.

ii. Citing machines often referred to as Universal Forensic Extraction Devices (UFEDs), petitioner contends that officers can preserve cell-phone data by blindly copying the entire contents of a cell phone at the scene of an arrest. That suggestion is entirely unrealistic. A modern UFED sold by the leading manufacturer (Cellebrite) costs about $10,000, and the cost of associated hardware and software "could go * * * far above" that amount. *Product Information: Cellebrite UFED Touch Ultimate*, SC Mag. (May 1, 2013) (*Cellebrite Review*).[11] Annual maintenance and upgrade costs may add another "few thousand dollars per license." Gogolin 44. And a police department must pay for special training for each officer who uses a UFED. See, *e.g.*, Digital Shield, Inc., *Cellebrite UFED Certified Training*.[12] It would thus be incredibly expensive to supply each of the 461,000 local police officers across the country with a UFED—to say nothing of the 120,000 full-time federal officers authorized to make arrests. See Bureau of Justice Statistics, *Local Police* (2008 statistics);[13] Bureau of Justice Statistics, *Federal Law Enforcement Officers* (2008 statistics).[14]

---

[11] www.scmagazine.com/cellebrite-ufed-touch-ultimate/review/3870.

[12] www.digitalshield.net/cellebriteinfo.php.

[13] www.bjs.gov/index.cfm?ty=tp&tid=71.

[14] www.bjs.gov/index.cfm?ty=pbdetail&iid=4372.

UFEDs, moreover, are not iPhone-sized tools that officers could keep in their pockets. Although handheld, they are fairly sizeable devices, and because different phones use different types of data ports, UFED kits include dozens of different cords. See App., *infra* (reproducing picture of a UFED kit). The notion that each officer in the field who might make an arrest should carry one of those kits wherever she patrols is wholly unworkable.

UFEDs have still other problems. They are unable to retrieve data from every phone. See Gogolin 48; Casey & Turnbull 19; Bennett, *supra*. Even for some common phones that are usually compatible with a UFED, the device may not work with all models and versions of the operating system. See Ronen Engler & Christa M. Miller, *6 Persistent Challenges with Smartphone Forensics*, Digital Forensic Investigator News (Feb. 8, 2013);[15] see also Gogolin 43. And even if the UFED works with a particular phone, that does not mean that it can extract every type of data on the phone. See Gogolin 58. Moreover, to function effectively, a UFED generally requires an officer to know the make, model, and service provider of the phone. NIST Draft Guidelines 38. That information may not be readily apparent from the exterior of the phone, particularly in a tense, nighttime arrest situation. *Id.* at 38-40. And the inexpensive disposable cell phones favored by drug dealers and terrorists (commonly known as "burner" phones) often lack the data ports necessary to use a UFED at all. Engler & Miller, *su-*

---

[15] www.dfinews.com/articles/2013/02/6-persistent-challenges-smartphone-forensics.

pra; Mobile Guide 6 ("With cheaper versions [of prepaid phones], there isn't always a means of copying data off the phone for an examination.").

Additionally, preserving the contents of a phone with a UFED is not instantaneous. An independent review of the most advanced Cellebrite device found that extracting certain types of information that would otherwise be readily viewable on the phone by an officer at the scene, such as text messages and call logs, takes between 2 and 15 minutes, depending on the phone. *Cellebrite Review*, *supra*. A forensic copy of the phone's contents takes at least 20 to 45 minutes. *Ibid.* Particularly when an arrest has not been planned and coordinated in advance, or where officers seize multiple phones from multiple arrestees, it will often be impracticable for an arresting officer to spend such time extracting data from a phone.

iii. Some of petitioner's amici suggest that remote wiping is not a real problem. See, *e.g.*, DKT Liberty Project Amicus Br. 34-35. But petitioner and his amici themselves point to federal and state law-enforcement guidelines instructing officers to take steps to prevent remote wiping, which would be puzzling if it posed no threat. See, *e.g.*, Pet. Br. 23 nn.8-9; see also, *e.g.*, Gogolin 59; Mislan at 113; Casey & Turnbull 3, 13. Although appellate decisions reporting remote wiping are unlikely (destroyed evidence cannot be introduced), such events occur. See Press Release, U.S. Attorney's Office, S.D. Ga., Martinez Man Sentenced to More Than 24 Years for Attempted Online Enticement of a Minor and Destruction of Evidence (Jan. 22, 2014) ("Shortly [a]fter [the suspect's arrest], he contacted his wife from jail and * * *

instructed her to delete his e-mail account and remotely wipe his phone.").[16]

c. Petitioner limits his discussion of *Chimel*'s officer-safety justification to the question whether cell-phone data can be used as a weapon. See Br. 16-19. But reviewing recent text messages or emails can alert officers that confederates or others are headed to the scene of an arrest, potentially creating a dangerous situation. See U.S. *Wurie* Br. 41-42.

d. Although petitioner suggests (Br. 20) that officers can quickly procure search warrants, "[e]ven with modern technological advances, the warrant procedure imposes burdens" and therefore "[w]hen a warrantless search is justified, requiring the police to obtain a warrant may 'unjustifiably interfer[e] with legitimate law enforcement strategies.'" *Fernandez* v. *California*, 134 S. Ct. 1126, 1137 (2014) (quoting *Kentucky* v. *King*, 131 S. Ct. 1849, 1860 (2011)) (third alteration in *Fernandez*). The search of items seized from an arrestee's person has historically been justified as a legitimate investigative procedure. And even with advances in obtaining warrants, delay in searching a cell phone poses a significant risk that evidence will be lost forever.

Finally, any claim to exempt cell phones from the traditional search-incident-to-arrest doctrine because of the supposed possibility of obtaining a warrant encounters a basic practical problem: cell phone technology is rapidly evolving, and unforeseen threats to such delayed searches may well emerge in the future.

---

[16] www.fbi.gov/atlanta/press-releases/2014/martinez-man-sentenced-to-more-than-24-years-for-attempted-online-enticement-of-a-minor-and-destruction-of-evidence.

Cf. *City of Ontario, Cal.* v. *Quon*, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."). It would be unwise to establish new and categorical constitutional limits on the police's traditional search authority based on a snapshot in time of a fast-changing technology.

B. Privacy Concerns Do Not Justify A Cell-Phone Exception To Officers' Search-Incident-To-Arrest Authority

Petitioner argues (Br. 24-38) that unique privacy concerns in cell phones justify a special exemption from officers' traditional search authority incident to lawful arrests. He fears (Br. 11) that every citizen will be subject to arrest at any time and that police will use such custodial arrests as pretexts to review individuals' private e-Book libraries and to probe their innermost "thoughts, wonders, and concerns."

That speculation has little connection to the arrests in this case and in *Wurie*: each involved probable-cause arrests for serious offenses, and the police conducted a search of the arrestees' cell phones to gather evidence relevant to the offense of arrest and to advance other vital law-enforcement objectives. The Court has no evidence that would justify treating these cases as atypical—or for fashioning a rule to address supposed abuses unrelated to these cases. Although cell phones can store more information than physical items such as diaries, address books, wallets, or purses, that characteristic is no reason to interpret the Fourth Amendment to deny officers a longstanding feature of their arrest authority, thereby ham-

stringing investigations as criminals have become more technologically sophisticated.

1. a. Petitioner contends (Br. 11) that because cell phones can contain a great deal of personal information, searching them is "the modern equivalent" of the sort of "general search" that the Fourth Amendment was adopted to prevent. But petitioner's central premise—that searching a cell phone incident to arrest "gives law enforcement the ability to obtain personal information formerly beyond its reach" (Br. 13)—is erroneous. Cell phones do not contain qualitatively different information than other sorts of items that courts have long permitted police to search incident to arrest. A cell phone can contain a list of contacts, but so can an address book. *E.g.*, *United States* v. *Smith*, 565 F.2d 292, 294 (4th Cir. 1977). Text messages and emails are modern-day letters. *E.g.*, *Dillon* v. *O'Brien & Davis*, 16 Cox C.C. 245, 248 (Exch. Div. Ir. 1887). And petitioner has cited no case holding that the police lack the power to examine photographs or other pictures found on an arrestee—often critical evidence of serious crimes, like the distribution of child pornography.[17]

---

[17] Petitioner suggests in passing (Br. 34 n.11) that this Court should overrule its longstanding precedent that a search may be conducted for "mere evidence" of crime, at least as to papers. But as this Court has held, "[n]othing in the language of the Fourth Amendment supports the distinction between 'mere evidence' and instrumentalities, fruits of crime, or contraband." *Warden* v. *Hayden*, 387 U.S. 284, 301 (1967). Petitioner cites no case or Founding-era source limiting the search of papers incident to a lawful arrest. And the law review article on which he relies acknowledges "a powerful argument that the original understanding did permit narrow, brief, and regulated seizures of papers.

The limited authority to search incident to arrest differs critically from general warrants, such as the hated writs of assistance. A "general warrant specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald* v. *United States*, 451 U.S. 204, 220 (1981); see *Wilkes* v. *Wood*, 98 K.B. 489, 498 (1763) (describing a "general warrant" as one "where no offenders[']] names are specified" and "therefore a discretionary power [is] given to messengers to search wherever their suspicions may chance to fall"). A search incident to arrest requires probable cause to arrest, and, as applied here, the search is limited to the person and objects found on his person at the time of arrest.

Cell phones do differ from objects that police have searched incident to arrest since the Founding era in their greater storage capacity: not different kinds of information, but potentially more of it. That concern does not justify dramatically curtailing officers' investigative tools. At least where, as here, the search occurs before "the administrative mechanics of arrest have been completed and the prisoner is incarcerated," *United States* v. *Edwards*, 415 U.S. 800, 804 (1974), officers could never review the entire contents of an arrestee's E-book library or peruse years' worth

---

Search upon arrest was a familiar feature of Founding-era practice" and "there is no known instance of a court holding the seizure of papers from an arrested person to be unconstitutional." Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 108 (2013).

of the arrestee's personal correspondence. Although in that period officers may be able to run searches on a collection of emails or other files for evidence of crime and review photos or contacts for potential criminal associations, the suggestion that officers will use that period to delve into the "thoughts, wonders, and concerns" of arrestees, rather than seek evidence and accomplish other legitimate law-enforcement objectives, is unfounded.

b. Petitioner also overstates what a warrant to search a cell phone would accomplish. He contends that a warrant would identify "which files to search, how far back in time to search, and which attachments or links to activate." Pet. Br. 31. But a warrant would not so specify. When the police show probable cause, the "place" to be searched is the cell phone, and the officers may search for evidence for which they have probable cause through "at least a cursory review of each file" on the phone that may contain the object of the search. *United States* v. *Williams*, 592 F.3d 511, 522 (4th Cir.) (computer search), cert. denied, 131 S. Ct. 595 (2010); see *Andresen* v. *Maryland*, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.").

A warrant requirement would foreclose searches where officers could not show probable cause to believe that a phone contains evidence of crime. But that is the type of search that the Fourth Amendment has long authorized for address books, wallets, purses, and papers on the arrestees' person because of his reduced expectation of privacy and the common-sense

intuition that evidence of an arrestee's crime is likely to be found on his person.

Finally, the risk that officers might abuse their authority and publicly disseminate sensitive information found on an individual's phone (Pet. Br. 37 n.12) also exists for a search under a warrant. The remedy for such isolated misconduct is internal discipline and possibly tort liability, not depriving all officers nationwide of their traditional search authority.

2. Petitioner also argues (Br. 31-38) that this Court should apply heightened Fourth Amendment scrutiny because "smart phones hold information that implicates First Amendment concerns." Pet. 31 (capitalization altered). As this Court has explained, however, "[t]here is no special sanctity in papers." *Gouled* v. *United States*, 255 U.S. 298, 309 (1921), overruled on other grounds by *Warden* v. *Hayden*, 387 U.S. 294 (1967). While "the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude'" when seized materials may have First Amendment protection, *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 564 (1978) (citation omitted), search-incident-to-arrest authority under the Fourth Amendment has *always* allowed the inspection of papers found on an arrestee's person. U.S. *Wurie* Br. 25-26.

Petitioner cites two sets of cases to support his novel limitation on search-incident-to-arrest authority. First, he cites (Br. 34-36) pre-*Chimel* search-incident-to-arrest cases analyzing whether a particular search of the *premises* of an arrest was reasonable. See Pet. Br. 34-35. That reasonableness standard, however, did not categorically insulate papers from officers' search authority. See *Hill* v. *California*, 401 U.S. 797, 799-802 & 800 n.1 (1971) (upholding search

of diary incident to arrest); *United States* v. *Bennett*, 409 F.2d 888, 897 (2d Cir.) (Friendly, J.) (cited at Pet. Br. 36) (upholding the warrantless review of letter "discovered in a lawful search of [arrestee's] pocketbook for narcotics * * * to see whether it was an 'instrumentality' for effecting the conspiracy"), cert. denied, 396 U.S. 852 (1969). In addition, the case on which petitioner places the greatest weight, *United States* v. *Lefkowitz*, 285 U.S. 452 (1932), rested primarily on the now-discredited view that, even under a warrant, officers lack authority to seize "mere evidence" of crime. See *id.* at 464-466; note 17, *supra*.

In any event, this Court has never suggested that officers' "unqualified authority" to search the person of the arrestee is diminished with respect to written material. *Robinson*, 414 U.S. at 225. Even in *Lefkowitz*, this Court did not cast doubt on the court of appeals' holding that the seizure of papers from the person of the arrestee was lawful. See 285 U.S. at 458, 461. As Judge Hand explained, "the law has never distinguished between documents and other property found upon the person of one arrested." *United States* v. *Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926).

Second, petitioner relies (Br. 33-34) on First Amendment cases involving the content-based seizure, under a warrant, of books or films. In *Marcus* v. *Search Warrant*, 367 U.S. 717 (1961), and *A Quantity of Copies of Books* v. *Kansas*, 378 U.S. 205 (1964), for example, "the material seized fell arguably within First Amendment protection, and the taking brought to an abrupt halt an orderly and presumptively legitimate distribution or exhibition." *Roaden* v. *Kentucky*, 413 U.S. 496, 504 (1973). The Court held that without

a valid warrant that described the allegedly unlawful media with sufficient specificity, the seizures constituted "a form of prior restraint." *Ibid.*; see *id.* at 506. The Court's central concern in the cases petitioner cites was the "use by government of the power of search and seizure as an adjunct to a system for the suppression of objectionable publications," *ibid.* (quoting *Marcus*, 367 U.S. at 724)—that is, the use of broad warrants to seize books and other material where "the basis for their seizure is the ideas which they contain," *Stanford* v. *Texas*, 379 U.S. 476, 485 (1965).

It trivializes that important principle to contend that the search of an arrestee's cell phone to find evidence of crime or to confirm his gang affiliation presents a "serious hazard of suppression of innocent expression." *Marcus*, 367 U.S. at 729; cf. *Roaden*, 413 U.S. at 505 (distinguishing seizures from commercial theatres from seizures where there is probable cause to arrest because "contraband is changing hands or * * * a robbery or assault is being perpetrated"). Petitioner does not even contend that his phone was unlawfully *seized*, defeating any analogy to prior-restraint cases, and in any event he makes no claim that the seizure inhibited him from disseminating expressive material to the public or that his phone was seized because of the content of his expression. No case of this Court has ever held that private correspondence and similar communicative content—often the most important evidence of criminal conspiracies—enjoys a special protection from police inquiry.

Finally, petitioner asserts (Br. 33-34) that searching an arrestee's phone for evidence impinges on associational freedoms. But for serious criminal offenses, investigating a suspect's associations—confederates,

suppliers, witnesses, victims—is basic police work. That everyday law-enforcement activity has no relationship to the restrictions on associational freedoms, such as the compelled disclosure of membership lists of law-abiding political associations, that this Court has condemned. Cf., *e.g.*, *NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449, 465 (1958) (distinguishing an organization engaged in "acts of unlawful intimidation and violence").

C. A Total Prohibition On Cell-Phone Searches Incident To Arrest Cannot Be Justified

1. In *Wurie*, the United States argues (Br. 45-49) that, if cell-phone searches incident to arrest were not thought categorically permissible under *Robinson*, the Court should at a minimum permit them when officers reasonably believe that a phone contains evidence of the offense of arrest. This Court adopted that standard in *Gant* for vehicle searches incident to arrest that do not sufficiently implicate the *Chimel* evidence-preservation and safety interests. See 556 U.S. at 335, 343.

Petitioner objects (Br. 38-43) to that proposal for two reasons, neither of which is sound. First, petitioner observes that *Gant* cited "circumstances unique to the vehicle context" in establishing its standard. 556 U.S. at 343. He speculates about the Court's concerns, but no need for speculation exists: the Court cited Justice Scalia's concurrence in *Thornton*, which explained that "motor vehicles" are "a category of 'effects' which give rise to a reduced expectation of privacy." 541 U.S. at 631. The same is true for objects found on the person of an arrestee. See *Chadwick*, 433 U.S. at 16 n.10; *Edwards*, 415 U.S. at 808-809; *Robinson*, 414 U.S. at 237 (Powell, J., concurring).

Justice Scalia derived that standard, moreover, primarily from the general interest in evidence-gathering that undergirded the search-incident-to-arrest doctrine as an original matter. See *Thornton*, 541 U.S. at 629-632.

Second, petitioner contends that under a *Gant*-based standard, "a curious police officer will virtually always be able to assure himself that he has reason to believe that an arrestee's smart phone contains evidence of the crime(s) of arrest" (Br. 42)—while arguing a page later that the standard is not met in this case. Petitioner's concern is unfounded. As with other Fourth Amendment doctrines that require officers to conduct on-the-scene reasonableness determinations (see, *e.g.*, *Terry* v. *Ohio*, 392 U.S. 1 (1968)), courts would develop guidelines about when officers can reasonably conclude that a phone is likely to contain evidence relevant to particular crimes, and suppression would be available where officers transgress those limits.

The United States has provided examples when a *Gant*-based standard would and would not be satisfied. See U.S. *Wurie* Br. 47-48. In particular, most traffic offenses would not justify a search of an arrestee's cell phone under that standard. (Petitioner cites no evidence supporting his speculation (Br. 41) that officers can determine the speed at which a motorist was driving from the locational information on a cell phone.) Likewise, officers could not search the phones of those arrested for "jaywalking, littering, or riding a bicycle the wrong direction." Pet. Br. 2. But petitioner's blanket prohibition on cell-phone searches would deprive officers of a longstanding tool even for serious offenses like drug trafficking and gang-related

violence. No Fourth Amendment justification compels that result.

2. The United States also suggested in *Wurie* (Br. 49-55) that if concern about the amount of private information contained on a cell phone persuades this Court to draw an item-specific exception from the *Robinson* categorical rule, it could address that concern by limiting the *scope* of any search in this context to the areas of the phone reasonably related to finding evidence relevant to the crime of arrest, identifying the arrestee, and protecting officers. Petitioner does not address such a scope-limited approach. But that approach would dispel the theoretical fears of vast "exploratory" searches raised by petitioner and his amici.

D. The Search Of Petitioner's Cell Phone Was Lawful

Under the settled search-incident-to-arrest doctrine articulated in *Weeks*, *Robinson*, and other decisions of this Court, officers had authority to search petitioner's cell phone after he was lawfully arrested. But the search was also valid under either of the narrower approaches suggested by the United States—a *Gant*-based standard or a scope-limited standard.

With respect to the first approach, the superior court found that the search "relat[ed] to the crime for which [petitioner] was arrested." J.A. 23. Officers had reason to believe that petitioner was a member of the Lincoln Park Bloods based on the paraphernalia he was carrying and that the phone might contain photographic evidence linking petitioner to the firearms for which he had been arrested. *Ibid.* Additionally, the offenses of arrest carried an enhancement if "the person is an active participant in a criminal street gang." Cal. Penal Code §§ 12025(b)(3), 12031(a)(2)(C)

(West 2008). It was reasonable to believe that his phone might contain evidence of his gang affiliation.

Similarly, under a scope-limited approach, the officers' review of texts, photos, and videos on petitioner's cell phone was reasonably related to discovering evidence of the crime of arrest and to the "identification and isolation of gang members before they are admitted" to a detention facility. *Florence* v. *Board of Chosen Freeholders*, 132 S. Ct. 1510, 1519 (2012). No evidence was introduced that fell outside of those categories. See 134 S. Ct. 999 (2014) (limiting question presented to whether "evidence admitted at petitioner's trial was obtained in a search * * * that violated petitioner's Fourth Amendment rights").

II. THE STATIONHOUSE SEARCH OF PETITIONER'S CELL PHONE OCCURRED WITHIN A REASONABLE TIME AFTER HIS ARREST

Petitioner argues that, even if officers had authority to search his phone, the second search at the stationhouse took place too long after his arrest to be justified as a search incident to that arrest. That contention lacks merit.

A. This Court held in *Edwards*, *supra*, that a search of the person incident to arrest may occur at the stationhouse rather than at the scene of arrest. In that case, the Court deemed a delay of ten hours in seizing the clothing of the arrestee and sending it to a laboratory for forensic analysis to be a "reasonable delay." 415 U.S. at 805. The Court explained that "both the person and the property in [an arrestee's] immediate possession may be searched at the station house after the arrest has occurred at another place and if evidence of crime is discovered, it may be seized and admitted in evidence." *Id.* at 803. That rule fol-

lows, the Court continued, from the basic principle that an arrest "for at least a reasonable time" takes the arrestee's "privacy out of the realm of protection from police interest in weapons, means of escape and evidence." *Id.* at 808-809 (citation omitted).

Petitioner would limit *Edwards* (Br. 49-51) to property still in a suspect's possession at the place of detention. *Edwards* did not rely on that fact. Nor can petitioner's view be reconciled with the Court's holding that objects seized at the place of detention could be "later subjected to laboratory analysis"—a search that, under petitioner's view, would be insufficiently contemporaneous with the arrest—or with the Court's statement that a search is permissible even if it occurs "at a later time" than the seizure. 415 U.S. at 804, 807. And contrary to petitioner's characterization (Br. 50), *Edwards* plainly applied the search-incident-to-arrest doctrine, not the inventory-search doctrine; the critical part of the Court's analysis was set forth before its brief discussion of *Cooper* v. *California*, 386 U.S. 58 (1967).

Importantly, *Edwards*'s holding applies to searches of the arrestee's *person* and items on his person—not items found near the location of arrest. The distinction flows from the different expectations of privacy. As discussed, *Chadwick* held that "[o]nce law enforcement officers have reduced * * * personal property *not immediately associated with the person of the arrestee* to their exclusive control," they no longer may search it without a warrant. 433 U.S. at 15 (emphasis added). But *Robinson* and *Edwards* rely on the arrestee's reduced expectations of privacy in his person for a different rule for searches of the person and his immediate possessions.

Like *Chadwick*, the two pre-*Edwards* decisions that petitioner cites—*Preston* v. *United States*, 376 U.S. 364 (1964), and *Dyke* v. *Taylor Implement Manufacturing Co.*, 391 U.S. 216 (1968)—concerned the search of an object found near the scene of arrest (the suspect's vehicle), not on the arrestee's person. And the leading circuit decision petitioner cites for his timing argument (Br. 47 n.16) explained, citing *Edwards* and *Chadwick*, that "[s]earches of the person and articles immediately associated with the person of the arrestee are treated differently" because "an arrest diminishe[s] one's expectation of privacy in one's person, thereby rendering reasonable any later search." *United States* v. *$639,558 in U.S. Currency*, 955 F.2d 712, 716 n.6 (D.C. Cir. 1992) (internal quotation marks and citation omitted) (search of 80-pound suitcase). Thus, at least where a search of items on the arrestee's person is conducted "a reasonable time" after the arrest, it is valid under *Edwards*. 415 U.S. at 809.

B. That approach makes practical sense. As discussed above, officers are entitled to conduct a full search of an individual upon arrest "to discover and seize the fruits or evidences of crime." *Robinson*, 414 U.S. at 224-225 (quoting *Weeks*, 232 U.S. at 392). That rule is justified in part because, in the aftermath of an arrest, the police must act quickly to apprehend confederates and quell threats to public safety. See U.S. *Wurie* Br. 30-31. But it may be unsafe or infeasible to conduct that search at the scene of arrest. It may be dark, or the weather may be bad; the officer may be dealing with multiple arrestees, witnesses, and victims; or the officer could perceive danger to herself or the arrestee. Thus, it is sensible to permit the officer, "for at least a reasonable time" after the arrest, to re-

tain the authority to conduct the evidentiary search that she could have conducted "on the spot at the time of arrest." *Edwards*, 415 U.S. at 803, 808-809.

Petitioner seeks (Br. 51-53) a phone-specific exception to *Edwards* on the ground that new data could be sent to the phone between the time of arrest and the time of the search. He offers no Fourth Amendment justification for that request. Information sent to the phone immediately after an arrest may be particularly likely to contain evidence of the crime of arrest—for example, a confederate's inquiry into the arrestee's whereabouts. Although an officer's affirmative use of a phone to view files stored elsewhere raises different privacy issues, that limitation is not implicated where other individuals transmit information to an arrestee's phone following an arrest. The arrestee's diminished expectation of privacy continues to justify a warrantless search of the phone.

Finally, petitioner errs in suggesting (Br. 52-53) that the search of a cell phone incident to arrest might violate Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2511-2522, or the Stored Communications Act, 18 U.S.C. 2701, 2703(a). Title III is not implicated when stored e-mails are accessed, because the interception is not "contemporaneous with transmission." *United States* v. *Steiger*, 318 F.3d 1039, 1047-1049 (11th Cir) (citing decision of two other circuits), cert. denied, 538 U.S. 1051 (2003). Likewise, it would not violate the Stored Communications Act to review any item stored on the phone itself. See *id.* at 1049. In any event, statutory restrictions do not define the Fourth Amendment's scope. *Quon*, 130 S. Ct. at 2632.

C. The stationhouse search in this case was valid. The search took place soon after petitioner arrived at the stationhouse and, as in *Edwards*, before "the administrative mechanics of arrest ha[d] been completed." 415 U.S. at 804; J.A. 15-16; Br. in Opp. 2. The delay, moreover, was reasonable. The initial search at the scene of arrest, including of petitioner's cell phone, revealed evidence of gang involvement, and the arresting officer brought in a detective specializing in gangs to interview petitioner and review his phone. As this Court has explained, the police have a substantial interest in identifying gang members as part of a custodial arrest. See *Florence*, 132 S. Ct. at 1519. A reasonably prompt search could also provide evidence to allow police to focus their investigation, locate witnesses or confederates, and anticipate any immediate repercussions in the community that the arrest might cause.

CONCLUSION

The judgment of the court of appeal should be affirmed.

Respectfully submitted.

DONALD B. VERRILLI, JR.
Solicitor General
DAVID A. O'NEIL
Acting Assistant Attorney General
MICHAEL S. DREEBEN
Deputy Solicitor General
JOHN F. BASH
Assistant to the Solicitor General
ROBERT A. PARKER
Attorney

APRIL 2014

(1a)

http://norhursttactical.com/training/professional-individual-training/advanced-mobile-forensics/

AMICUS CURIAE BRIEF

RECORD AND BRIEFS

No. 13-132

Supreme Court, U.S.
FILED
MAR - 7 2014
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

—v.—

STATE OF CALIFORNIA,

Respondent.

ON WRIT OF CERTIORARI TO THE CALIFORNIA COURT OF APPEAL, FOURTH APPELLATE DISTRICT

BRIEF OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, THE AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, AND THE AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO AND IMPERIAL COUNTIES AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

Linda Lye
American Civil Liberties
Union Foundation of
Northern California
39 Drumm Street, 2nd Floor
San Francisco, CA 94111

Susan N. Herman
Counsel of Record
250 Joralemon Street
Brooklyn, NY 11201
(718) 780-7945
susan.herman@brooklaw.edu

Steven R. Shapiro
Ezekiel R. Edwards
Catherine Crump
American Civil Liberties
Union Foundation
125 Broad Street
New York, NY 10004

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF AMICI 1

SUMMARY OF ARGUMENT 1

ARGUMENT 5

I. ALLOWING WARRANTLESS SEARCHES OF CELL PHONES INCIDENT TO ARREST UNDERMINES FUNDAMENTAL FOURTH AMENDMENT PRINCIPLES 5

A. "Papers" And "Effects" That Were Previously Stored In Our "Houses" And Protected By The Fourth Amendment Are Now Stored On Our Cell Phones 5

B. Fourth Amendment Limitations on the Power to Arrest Are Insufficient to Protect the Privacy of the Papers and Effects Contained in Cell Phones. 9

II. THE FOURTH AMENDMENT REQUIRES A SEARCH WARRANT BEFORE ANY SEARCH OF A CELL PHONE OR OTHER PORTABLE ELECTRONIC DEVICE 16

A. The Expectation of Privacy in One's Papers and Effects Is Not Abated by the Fact of an Arrest 16

B. A Per Se Rule Prohibiting Cell Phones Searches Absent A Warrant Or Exigent Circumstances Is More Easily Administrable Than Alternative Approaches 20

III. CELL PHONES ARE ENTITLED TO HEIGHTENED PROTECTION UNDER THE FOURTH AMENDMENT BECAUSE THEY CONTAIN FIRST AMENDMENT-PROTECTED ASSOCIATIONAL INFORMATION 26

A. This Court Has Long Recognized That The First Amendment Protects The Right To Associate In Private 28

B. Cell Phones Contain A Substantial Amount Of Associational Material 29

CONCLUSION 36

TABLE OF AUTHORITIES

CASES

Arizona v. Gant,
556 U.S. 332 (2009) ..... *passim*

Atwater v. City of Lago Vista,
532 U.S. 318 (2001) ..... *passim*

Barnett v. United States,
525 A.2d 197 (D.C. 1987) 13

Boyd v. United States,
116 U.S. 616 (1886) 5

Brown v. Socialist Workers '74 Campaign Comm. (Ohio), 459 U.S. 87 (1982) 29

Carroll v. United States,
267 U.S. 132 (1925) 24

Chimel v. California,
395 U.S. 752 (1969) 2, 8, 19, 20

City of Ontario, Cal. v. Quon,
560 U.S. 746 (2010) 23

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 8

Devenpeck v. Alford,
543 U.S. 146 (2004) 10

Dinler v. City of New York, 2012 U.S. Dist. LEXIS 141851 (S.D.N.Y. Sept. 30, 2012) 15

Entick v. Carrington, 19 How. St. Tr. 1029 (C.P.) (Eng.) (1765) 2, 5, 6, 19

Harris v. United States,
331 U.S. 145 (1947) 35

In re Alfredo C.,
2011 WL 4582325 (Cal. Ct. App. Oct. 5, 2011)..... 12

Kyllo v. United States,
533 U.S. 27 (2001) 8, 9

Maryland v. King,
___ U.S. ___, 133 S. Ct. 1958 (2013)..... 17

Maryland v. Macon,
472 U.S. 463 (1985) 27

Missouri v. McNeely,
___ U.S. ___, 133 S. Ct. 1552 (2013)..... 16

NAACP v. Alabama,
357 U.S. 449 (1958) 28, 31

NAACP v. Button,
371 U.S. 415 (1963) 31

Newhard v. Borders,
649 F. Supp. 2d 440 (W.D. Va. 2009)..... 13, 14

Offer-Westort v. City & Cnty. of S.F., 2013 WL
1149257 (Cal. Super. Mar. 20, 2013) 34, 35

Olmstead v. United States,
277 U.S. 438 (1928) 24, 35, 36

Payton v. New York,
445 U.S. 573 (1980) 5, 6, 8

People v. Diaz, 244 P.3d 501, *cert. denied*, 132 S. Ct.
94 (2011).....*passim*

People v. Killion, 2012 WL 6604981 (Cal. Ct. App.
Dec. 19, 2012), *rev. denied*, (Feb. 27, 2013) 12

Reno v. ACLU,
521 U.S. 844 (1997) 30

Robinson v. United States,
414 U.S. 218 (1973) ..... *passim*

Schlossberg v. Solesbee,
844 F.Supp.2d 1165 (D. Or. 2012) 15

Shelton v. Tucker,
364 U.S. 479 (1960) 28, 29

South Dakota v. Opperman,
428 U.S. 364 (1976) 24, 25

Stanford v. Texas,
379 U.S. 476 (1965) 5, 8

State v. Granville, 2014 WL 714730 (Tex. Crim. App.
Feb. 26, 2014) 13

State v. Smith,
920 N.E.2d 949 (2009) 16, 17, 23

Thomas v. Florida,
614 So.2d 468 (Fla. 1993) 13

Thornton v. United States,
541 U.S. 615 (2004) 19, 21

United States v. Chadwick, 433 U.S.1 (1977),
partially abrogated by California v. Acevedo,
500 U.S. 565 (1991) ..... *passim*

United States v. Edwards,
415 U.S. 800 (1974) 18

United States v. Flores-Lopez,
670 F.3d 803 (7th Cir. 2012) 23

United States v. Holzman,
871 F.2d 1496 (9th Cir. 1989) 23

United States v. Lefkowitz,
285 U.S. 452 (1932) 19

United States v. Murphy,
553 F.3d 405 (4th Cir. 2009) 23

United States v. Valdez,
2008 WL 360548 (E.D. Wis. Feb. 8, 2008) 23

United States v. Watson,
423 U.S. 411 (1976) 3, 9, 14, 20

United States v. Wurie, 728 F.3d 1 (1st Cir 2013),
cert. granted, 134 S.Ct. 999 (2014)..... 24

Virginia v. Moore,
553 U.S. 164 (2008) 9, 10, 14

Watkins v. United States,
354 U.S. 178 (1957) 28

Whren v. United States,
517 U. S. 806 (1996) 3, 9, 14

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 27

CONSTITUTION AND STATUTES

U.S. Const. amend I.....*passim*

U.S. Const. amend IV .....*passim*

Tex. Transp. Code Ann. § 543.001 (2013) 10

Va. Code Ann. §19.2-74 (2013) 10

Walnut City Code, Title III, Ch 17-31 § 4237.1..... 26

OTHER AUTHORITIES

Aaron Smith & Maeve Duggan, The State of the 2012 Election—Mobile Politics, Pew Research Center (Oct. 9, 2012)..... 31, 32

Aaron Smith, *Cell Internet Use 2012*, Pew Research Internet Ctr. (June 26, 2012) 8

Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. Rev. 27 (2008)..... 11, 22

Alexander Bolton, *Conservative Group Makes $1M High-Tech Investment to Help Tea Party*, The Hill (Apr. 12, 2012) 33

American Civil Liberties Union, *The War on Marijuana in Black and White* (2013) 14

Bob Samuels, *Facebook, Twitter, YouTube—and Democracy*, 97 Academe (2011)..... 32

Bryan Denson, *Eugene Verdict Clarifies Legal Protections for Protesters Who Turn Video Cameras on Police,* Pacific Northwest News (Jan. 29, 2012) 15

Declan McCullagh, *Police Push for Warrantless Searches of Cell Phones*, CNET NEWS (Feb. 18, 2010, 4:00 AM)..... 13

Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49 (2013)..... 17

Federal Bureau of Investigation, *Estimated Number of Arrests, Crime in the United States 2011* 12

Federal Bureau of Investigation, *Persons Arrested, Crime in the United States 2011* 11, 12

LA Archdiocese Launches Pro-Life Networking App, Cath. News Agency (Jan. 23, 2014) 34

Linda Greenhouse, *Divided Justices Back Full Arrests on Minor Charges*, N.Y. Times, Apr. 25, 2001..... 10

Lynn Langton & Matthew Durose, *Police Behavior during Traffic and Street Stops, 2011*, U.S. Department of Justice (Sept. 2013), ... 11

M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave it Birth*, 85 N.Y.U. L. Rev. 905 (2010)..... 35

Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L. Rev. 183 (2010)..... 22

Michael C. Gizzi, *Pretextual Stops, Vehicle Searches, and Crime Control: An Examination of Strategies Used on the Frontline of the War on Drugs*, 24 Criminal Justice Studies 139 (2011)..... 13

Michael DeGusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, MIT Tech. Rev. (May 9, 2012)..... 7

New York Civil Liberties Union, *Arresting Protest: A Special Report of the New York Civil Liberties Union on New York City's Protest Policies at the February 15, 2003 Antiwar Demonstration in New York City* (April 2003) 15

Nick Wingfield, *The Numbers Behind Twitter*, N.Y. Times, Oct. 3, 2013..... 31

Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J. L. & Pub. Pol'y 403 (2013)... 17

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) 26

Telford Taylor, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION (1969) 20

Tracey Maclin, *Annex Perspectives: Cell Phones, Search Incident to Arrest, and the Supreme Court*, 94 B.U.L. Rev. 3 (2014) 20

Vindu Goel, *Big Profit at Facebook as It Tilts to Mobile*, N.Y. Times, Jan. 29, 2014 31

Wayne R. LaFave, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (2012) 11, 20, 23

William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 Mich. L. Rev. 505 (2001) 12

William Tudor, THE LIFE OF JAMES OTIS (1823) 6

Zusha Elinson, *After Cellphone Action, BART Faces Escalating Protests*, N.Y. Times, Aug. 20, 2011 ... 33

INTEREST OF AMICI[1]

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil rights laws. Since its founding in 1920, the ACLU has appeared in numerous cases before the Supreme Court, both as direct counsel and as *amicus curiae*. This case raises an issue of particular importance to the ACLU: the application of Fourth Amendment safeguards to evolving technology that also implicates important First Amendment rights. We therefore submit this brief on behalf of the ACLU and its three California affiliates.

SUMMARY OF ARGUMENT

The ACLU submits this brief to make two principal points. First, given the absence of any meaningful limits on the power to arrest based on probable cause, it is critical for this Court to create some back-end safeguards to ensure that the search-incident-to-arrest doctrine does not allow the police to rummage through our most personal effects without constraint and without a warrant. Second, the Fourth Amendment interests in this case are heightened because cell phones contain both

---

[1] The parties have submitted blanket letters of consent to the filing of *amicus* briefs in this case. None of the parties authored this brief in whole or in part, and no one other than *amici* and its counsel made a monetary contribution to the preparation or submission of this brief.

expressive material and associational activity protected by the First Amendment.

1. Anglo-American houses and the papers and effects they contain have always commanded the most vigilant protection, even before the Fourth Amendment. *See Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P.) (Eng.) (1765). An officer who wants to search the papers and effects in our homes or offices may not do so without a search warrant. A neutral and detached magistrate must review the existence of probable cause and specify with particularity where the officer may search and what may be seized, preventing officers from ransacking our libraries and personal effects. *See, e.g., Chimel v. California*, 395 U.S. 752 (1969).

Cell phones and other portable electronic devices are, in effect, our new homes. They can contain voluminous quantities of information about the most intimate details of our lives, "papers and effects" of the sort that earlier generations of Americans kept in the bureaus and cabinets of their houses: correspondence (personal texts and emails), records of our commercial transactions and political activities, photographs, contact lists revealing our associations, and access to our activities on the internet and in the cloud. Especially for younger generations, the importance of the worlds of their portable electronic devices rivals the importance of their physical dwellings.

Extending the search-incident-to-arrest exception to the warrant requirement to allow a search of any cell phone accompanying an arrestee would permit circumvention of these fundamental safeguards and open a back door to our most private

papers and effects – indeed to our virtual homes – even when there is no probable cause to search. Police officers, rather than neutral magistrates, would determine whether such a search takes place and how invasive it would be. The only prerequisite to these general searches would be an arrest based on probable cause to believe the target has committed an offense. But this is a feeble protection, given the range of conduct that has been and can be declared unlawful, including minor offenses such as littering, jaywalking, creating a disturbance on a school bus, riding a bicycle without a bell or gong, disobeying police orders at a parade, and all traffic infractions.

Other than the requirement of probable cause, the Fourth Amendment imposes neither objective nor subjective limitations on the power to arrest. Arrests conducted outside the physical home may be made without a warrant, *see United States v. Watson*, 423 U.S. 411 (1976), so no magistrate will have reviewed even whether there is probable cause to arrest. Custodial arrests for minor, fine-only offenses like a seat belt violation are allowed. *See Atwater v. City of Lago Vista*, 532 U.S. 318 (2001). And, it is irrelevant under Fourth Amendment law that an officer has conducted an arrest as a pretext in order to search a target's cell phone. *See Whren v. United States*, 517 U. S. 806 (1996). Given the absence of front-end protections, this Court should adopt a *per se* rule that, absent exigent circumstances, a cell phone seized incident to arrest can only be searched pursuant to a warrant.

There is no effective and administrable alternative to the warrant requirement. Proposals to

dispense with warrants in some but not all cell phone searches, whether based on the type of device involved or the type of evidence reviewed, draw arbitrary lines that would often be difficult for officers or courts to apply. Allowing a search for evidence of the offense of arrest, an exception adopted in the context of searches of vehicles where there is a reduced expectation of privacy, *see Arizona v. Gant*, 556 U.S. 332 (2009), is not justifiable where our most intimate information is at stake. Furthermore, attempting to impose limiting conditions on searches of cell phones would be ineffectual when officers will decide for themselves how to apply those limits, and would create vexing questions about what parts of the phone's contents should then be considered to be in plain view.

2. The importance of requiring the police to obtain a warrant before searching a cell phone seized incident to arrest is heightened by the First Amendment interests at stake. Cell phones not only provide a means for expression, they contain substantial information about our constitutionally protected associations. Even basic cell phones contain contact lists and call histories, while Internet-enabled smart phones permit their users to access social networking applications that facilitate a panoply of associational activities. A substantial number of Americans use cell phones to send and receive information related to political campaigns. Cell phones have also become a crucial means for organizing political demonstrations and other forms of political action. In this context, the Fourth Amendment's warrant requirement provides an indispensable safeguard for fundamental First Amendment rights.

ARGUMENT

I. ALLOWING WARRANTLESS SEARCHES OF CELL PHONES INCIDENT TO ARREST UNDERMINES FUNDAMENTAL FOURTH AMENDMENT PRINCIPLES.

A. "Papers" And "Effects" That Were Previously Stored In Our "Houses" And Protected By The Fourth Amendment Are Now Stored On Our Cell Phones.

In *Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P.) (Eng.) (1765), the historic case described by this Court as the "wellspring" of the rights now protected by the Fourth Amendment, *see Stanford v. Texas*, 379 U.S. 476, 483-84 (1965), *Boyd v. United States*, 116 U.S. 616, 626-627 (1886), Lord Camden declared that John Entick's private papers and books could not be searched pursuant to a general warrant despite the fact that a warrant for his arrest had been issued. "Papers are the owner's dearest property," he said. *Entick*, 19 How. St. Tr. at 1066. "[I]f this point should be determined in favor of the jurisdiction, the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel." *Id.* at 1063.

James Otis, arguing against the despised writs of assistance, the immediate evil that inspired the framers of the Fourth Amendment to protect our "persons, houses, papers, and effects" against unreasonable searches and seizures, *see, e.g., Payton*

v. New York, 445 U.S. 573, 583-84 & n.21 (1980), echoed Lord Camden's fear of enabling oppressive government intrusion into private realms by "plac[ing] the liberty of every man in the hands of every petty officer," William Tudor, THE LIFE OF JAMES OTIS 66 (1823) –today, not just the Secretary of State's messengers but legions of federal, state, and local law enforcement officers who wield enormous discretionary power to arrest without a warrant.

A central reason for the special protection of the home is that our home cabinets, desks, bookshelves, and bureaus traditionally have been the principal repository of our most intimate papers and effects. The correspondence, diaries, address books, commercial records, portraits, books and pamphlets contained in the home can expose all essential aspects of a person's private life, politics, religion, and associations. As Entick's counsel had argued: "Has a secretary of state a right to see all a man's private letters of correspondence, family concerns, trade and business? This would be monstrous indeed! And if it were lawful, no man could endure to live in this country." *Entick*, 19 How. St. Tr. at 1038.

Smartphones and other portable electronic devices are the equivalent of the cabinets, desks, bookshelves, and bureaus in an eighteenth century home.[2] As detailed in other briefs, they contain

---

[2] The security of not only cell phones but a range of smartphones, laptops, thumb drives, and other portable electronic devices is at issue in this case. "Cell phone," the term used in the Question Presented, is being used here as shorthand to refer to the entire range of portable electronic devices capable of storing personal information, which we argue should be

massive quantities of emails and texts (today's letters), personal notes (today's diaries), contact lists (today's address books), reading materials (today's bookshelves), photographs and videos, call logs and voicemails, records of commercial transactions, access to internet browsers showing the owner's range of interests and commercial, political, charitable, and personal habits – and access to the world of information the phone's owner has stored on the cloud. These troves of electronic papers and effects are simply not comparable to other items that might be found in an arrestee's home, suitcase, or pocket.

A world of information about an individual's thoughts, associations, activities, and politics, formerly accessible only by searching the papers and effects in someone's house, is no longer hidden behind physical walls. But the protection provided by the Fourth Amendment for our private papers and effects does not become any less essential simply because we now carry so many of our papers and effects electronically outside our homes.[3]

---

treated alike, *see* Point II *infra*. It should be noted that the decision in this case may also affect how extensively a desktop computer, in addition to a cell phone, laptop, etc., in an arrestee's grabbable area, may be searched incident to an arrest in one's home or office.

[3] Americans—especially young Americans—are adopting smart phones at an unprecedented rate. Michael DeGusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, MIT Tech. Rev. (May 9, 2012), available at http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/. Non-Caucasians and youths—groups that experience proportionately higher arrest rates—are also especially likely to

This Court has rigorously implemented the Fourth Amendment's protection of the privacy of our houses and the papers and effects they contain by requiring 1) that searches of the home be preceded by a search warrant so that a neutral and detached magistrate can determine before the search whether or not probable cause in fact exists, *Coolidge v. New Hampshire*, 403 U.S. 443, 477-78 (1971); 2) that the scope of searches, especially of one's books and papers, be limited by a magistrate's particular description in the search warrant of what may be searched or seized, *Stanford v. Texas*, 379 U.S. 476, 485-86 (1965); 3) that the scope of any search incident to arrest in a home be carefully circumscribed so as not to become an unwarranted search of the contents of the home, *Chimel v. California*, 395 U.S. 752, 762-63 (1969); 4) that officers must obtain an arrest warrant to conduct an arrest in the home, even though arrests outside the home may be made on an officer's unreviewed assessment of probable cause, *see Payton v. New York*, 445 U.S. 573, 589-90, 602-03 (1980); and 5) that the permissibility of using technology to obtain information from inside a home without a warrant be measured, in part, by whether the intimate details at issue would otherwise have been discoverable only by a physical intrusion into the home, *Kyllo v. United States*, 533 U.S. 27, 34, 40 (2001) ("This assures preservation of that degree of privacy against

---

use their cell phones for the majority of their online activity. Aaron Smith, *Cell Internet Use 2012*, Pew Research Internet Ctr. (June 26, 2012), available at http://www.pewinternet.org/2012/06/26/cell-internet-use-2012/.

government that existed when the Fourth Amendment was adopted." *Id.* at 34.)

Our electronic worlds, in a very real sense, *are* our new homes and our Fourth Amendment traditions demand that they be respected as such.

B. Fourth Amendment Limitations on the Power to Arrest Are Insufficient to Protect the Privacy of the Papers and Effects Contained in Cell Phones.

United States v. Watson, 423 U.S. 411, 416-18, 423-24 (1976), ruled that no warrant is required for an arrest, at least outside the home, because there was no such requirement at common law. Justice Powell explained this apparently anomalous result – requiring the protection of warrants before searches but not before the arguably greater intrusion of arrest – as an example of logic deferring to history. *Id.* at 428 (concurring opinion). "There is no historical evidence," he said, "that the Framers or proponents of the Fourth Amendment, outspokenly opposed to the infamous general warrants and writs of assistance, were at all concerned about warrantless arrests by local constables and other peace officers." *Id.* at 429 (citation omitted).

Building on that premise, the Court's decisions in *Robinson v. United States*, 414 U.S. 218, 235 (1973), combined with the subsequent decisions in *Atwater v. City of Lago Vista*, 532 U.S. 318 (2001), *Virginia v. Moore*, 553 U.S. 164 (2008), and *Whren v. United States*, 517 U. S. 806 (1996), free federal, state, and local officers to arrest individuals for a vast array of minor offenses, thereby triggering

automatic authority to search incident to that arrest, even if the arrest itself was not permitted under state law, or was motivated solely by a desire to view the contents of the arrestee's cell phone.

In *Atwater*, *supra*, a divided Court declined to adopt a Fourth Amendment rule prohibiting custodial arrests for non-jailable offenses. Accordingly, the Court upheld Gail Atwater's custodial arrest for a fine-only seat belt violation based on probable cause, *see id.* at 323-24, which precipitated a fruitless search incident to arrest, *see* Linda Greenhouse, *Divided Justices Back Full Arrests on Minor Charges*, N.Y. Times, Apr. 25, 2001, http://www.nytimes.com/2001/04/25/us/divided-justices-back-full-arrests-on-minor-charges.html.

In some states, individuals can be taken into custody in connection with any or all traffic offenses, at the discretion of the officer. *See* Tex. Transp. Code Ann. § 543.001 (2013). Other states restrict their officers' discretion to arrest, *see, e.g.*, Va. Code Ann. §19.2-74 (2013), but the Court has held that the Fourth Amendment's search-incident-to-arrest exception does not require that the predicate arrest be valid under state law – only that there be probable cause, *see Virginia v. Moore*, 553 U.S. at 171 – magnifying the number of predicate arrests potentially at issue.[4]

Given the largely unbridled power to arrest and the lack of any limit on the accompanying

---

[4] *Devenpeck v. Alford*, 543 U.S. 146, 152-56 (2004), further widened the net by finding an arrest to be reasonable if the officer had probable cause to believe that any offense had been committed even if that offense was not what the officer had in mind.

authority to search at least the person of the arrestee, it is not surprising that searches incident to arrest now apparently constitute the largest exception to the search warrant requirement. *See* Wayne R. LaFave, 3 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §5.2(c) & n.55 (2012) (describing the search incident to arrest as probably the most common type of police search); *see also* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. Rev. 27, 31 (2008) (commenting on the connection between expansive criminal codes and the frequency of searches incident to arrest). Because the power to arrest for traffic and other minor offenses is unlimited by the Fourth Amendment except for the prerequisite of probable cause, a large percentage of the population is subject to arrest at any time. Data for 2011 show that over 62.9 million U.S. residents age sixteen or older, or twenty-six percent of the population, had one or more contacts with police during the prior twelve months. Traffic stops were a very common form of police contact in 2011. Ten percent of the 212.3 million U.S. drivers age sixteen or older (about twenty-one million) were stopped while operating a motor vehicle in 2011. *See* Lynn Langton & Matthew Durose, *Police Behavior during Traffic and Street Stops, 2011* (Sept. 2013), *available at* http://www.bjs.gov/content/pub/pdf/pbtss11.pdf.[5] Millions of Americans are arrested every year for committing misdemeanors.[6]

---

[5] The data do not show how many of these individuals were arrested for those offenses or how many could have been.

[6] According to the Uniform Crime Reports (UCR), law enforcement nationwide made an estimated 12,408,899 arrests in 2011 (not including traffic citations). *See Persons Arrested,*

The probable cause requirement alone offers feeble protection for liberty or privacy because legislatures define so much conduct as criminal. *See* William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 Mich. L. Rev. 505, 507 (2001) (discussing how the expanded, extraordinary breadth of American criminal law legislation has left the real boundaries of law to be defined by those who enforce it). Since the California Supreme Court decided in *People v. Diaz*, 244 P.3d 501, *cert. denied*, 132 S. Ct. 94 (2011), that it is permissible to search a cell phone incident to arrest, numerous California cases show similar fact patterns: an arrest for a traffic or other minor offense followed by a cell phone search leading to more serious charges. *See, e.g., People v. Killion*, 2D CRIM. B239876, 2012 WL 6604981 (Cal. Ct. App. Dec. 19, 2012), *rev. denied*, (Feb. 27, 2013) (not designated for publication) (traffic arrest; cell phone search leading to drug prosecution); *In re Alfredo C.*, B225715, 2011 WL 4582325 (Cal. Ct. App. Oct. 5, 2011) (graffiti arrest; digital camera search leading to firearms prosecution).

Crime in the United States 2011, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/persons-arrested/persons-arrested. Of these, almost 2 million (1,960,807) were for disorderly conduct, drunkenness, violations of liquor laws, vandalism, curfew and loitering law violations, and vagrancy. *See Estimated Number of Arrests, Crime in the United States 2011*, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/tables/table-29. An additional 3,532,195 were classified as "all other offenses", *Id.*, many if not most of which were other minor offenses.

This phenomenon is not confined to California. *See, e.g., State v. Granville*, No. PD-1095-12, 2014 WL 714730 (Tex. Crim. App. Feb. 26, 2014) (cell phone of high school student arrested for creating a disturbance on a bus searched at jail, leading to additional prosecution); *Thomas v. Florida*, 614 So.2d 468 (Fla. 1993) (search incident to arrest for riding a bicycle without a bell or gong leading to prosecution on other grounds); *Barnett v. United States*, 525 A.2d 197, 198 (D.C. 1987) (search incident to arrest for "walking as to create a hazard" leading to prosecution on other grounds). *See also* Michael C. Gizzi, *Pretextual Stops, Vehicle Searches, and Crime Control: An Examination of Strategies Used on the Frontline of the War on Drugs*, 24 Criminal Justice Studies 139 (2011) (study showing traffic stops leading to drug convictions were overwhelmingly discretionary and seemingly pretextual).

Even if no evidence of criminality is found, the "incidental" search of cell phones radically increases the potential consequences of an arrest. When Nathan Newhard, for example, was arrested for driving while intoxicated, *see* Declan McCullagh, *Police Push for Warrantless Searches of Cell Phones*, CNET NEWS (Feb. 18, 2010, 4:00 AM), http://news.cnet.com/8301-13578_3-10455611-38.html, a search of the cell phone he carried revealed nude photos of him with his girlfriend in sexually explicit positions. *Newhard v. Borders*, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009). A police sergeant shared these intimate photos with various officers, deputies, and members of the public "for their viewing and enjoyment." *Id.* The resulting

scandal led to Newhard losing his job as a school teacher.

Finally, there is no Fourth Amendment limitation on the use of pretextual arrests, *see Whren*, 517 U.S. at 813 (finding no subjective limit to the arrest power). The confluence of *Robinson*, *Atwater*, *Moore*, and *Watson* with *Whren* creates ample opportunity for any officer so inclined to orchestrate an arrest motivated only by the desire to trawl through the contents of someone's cell phone or electronic device. This virtual blank check creates a perverse incentive for officers to abuse the arrest power even where they do not believe an arrest would otherwise be desirable, transforming the search incident to arrest into an arrest incident to a search. An officer need only wait for a target to commit a traffic offense, or jaywalk, or fail to comply with technical parade permit or leafleting restrictions. Inevitably, some officers will use this vast discretionary power for troubling reasons: political, personal, prejudiced, or even prurient, as in *Newhard*.

It is impossible to document the full extent of the problem of arbitrary or discriminatory arrests because the relevant data are not gathered nationally. We do know, however, that aggressive use of discretionary police power leads to racially discriminatory results. *See, e.g.*, American Civil Liberties Union, *The War on Marijuana in Black and White* (2013), https://www.aclu.org/criminal-law-reform/war-marijuana-black-and-white-report (Blacks are 3.73 times as likely to be arrested for marijuana possession despite comparable usage rates). It can also have significant First Amendment

consequences. *See* Point III, *infra*. If an officer wants to search a political activist's cell phone, it is all too easy to find or manufacture a basis for arresting political demonstrators. [7]

If an increasingly consequential license to conduct searches of a person's private world can evade the tethers of the warrant requirement by disguising itself as a mere incident to arrest, the back door to our cyber-homes stands open.

---

[7] *See, e.g.*, New York Civil Liberties Union, *Arresting Protest: A Special Report of the New York Civil Liberties Union on New York City's Protest Policies at the February 15, 2003 Antiwar Demonstration in New York City* (April 2003) at 10, https://www.aclu.org/files/FilesPDFs/nyclu_arresting_protest1.pdf (over 350 people arrested at Feb. 15, 2003 antiwar demonstration in New York City, amid confusion about the parade route and police use of barricades); *Dinler v. City of New York*, 2012 U.S. Dist. LEXIS 141851 * 23-50 (S.D.N.Y. Sept. 30 2012) (mass arrests of demonstrators at 2004 Republican National Convention for blocking the sidewalk, parading without a permit – for deviating from prescribed route – and disobeying police orders).

Josh Schlossberg, an Oregon environmental activist, was arrested for using his electronic camera to record his encounter with an officer who was interrogating him about his leafleting activities. *See* Bryan Denson, *Eugene Verdict Clarifies Legal Protections for Protesters Who Turn Video Cameras on Police*, Jan. 29, 2012, http://www.oregonlive.com/pacific-northwest-news/index.ssf/2012/01/eugene_verdict_clarifies_law_p.html. This arrest provided the occasion for the officer to seize the camera and review the contents of the video without obtaining a search warrant. *Schlossberg v. Solesbee*, 844 F.Supp.2d 1165 (D. Or. 2012).

II THE FOURTH AMENDMENT REQUIRES A SEARCH WARRANT BEFORE ANY SEARCH OF A CELL PHONE OR OTHER PORTABLE ELECTRONIC DEVICE.

A. The Expectation of Privacy in One's Papers and Effects Is Not Abated by the Fact of an Arrest.

Given the permissive state of constitutional law regarding arrests, there is no meaningful check available on unwarranted intrusion into our private enclaves other than categorically prohibiting the warrantless search of a cell phone's papers and effects seized incident to arrest.

The California Supreme Court maintains that a bright line rule allowing searches of cell phones incident to arrest is justifiable under this Court's decision in *Robinson, supra*. *See Diaz, supra*. But this Court has held that warrantless intrusions are justifiable only when privacy interests are reduced or the historical record supports an exception to the warrant requirement. As this Court recently said in *Missouri v. McNeely*, ___ U.S. ___, 133 S. Ct. 1552, 1564 (2013), "While the desire for a bright-line rule is understandable, the Fourth Amendment will not tolerate adoption of an overly broad categorical approach that would dilute the warrant requirement in a context where significant privacy interests are at stake."

The privacy interests at stake in the context of cell phones searches are profound and dramatically more significant than could have been imagined in the eighteenth century or even in the 1973 world of *Robinson*. *See State v. Smith*, 920 N.E.2d 949, 955

(2009); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J. L. & Pub. Pol'y 403, 404-06 (2013). Forty years ago, the search of effects could plausibly be described as merely incidental to the greater intrusion of an arrest. *See, e.g, United States v. Chadwick*, 433 U.S.1, 20 (1977), *partially abrogated by California v. Acevedo*, 500 U.S. 565 (1991) (Blackmun, J., dissenting). That characterization has become implausible today when the question is whether to give the police easy access to the contents of a virtual library of information..

The *Robinson* Court held that the expectation of privacy in one's *person* is necessarily abated by a lawful arrest. *Id.* at 237-38 (Powell, J., concurring); *see also Maryland v. King*, ___ U.S. ___, 133 S. Ct. 1958, 1979 (2013). But the Court did not hold that the expectation of privacy in one's *effects* is so reduced by an arrest that any search of an arrestee's effects is justified simply by the desire to find evidence – certainly not where the effects contain as much revealing information as a cell phone. *See* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 53 (2013) ("legitimate textual and historical grounds [exist] for "treating 'papers' and their modern counterparts with more respect than other 'effects.'"). In ruling that the Fourth Amendment did not prohibit the search of a cigarette pack that had been removed from Robinson's pocket incident to arrest, the Court emphasized that the arresting officer might reasonably have feared that the pack contained a dangerous razor blade or (as it did) destructible contraband. 414 U.S. at 223. The Court expressed its unwillingness to require officers

to put themselves at risk by forcing them to guess whether or not an arrestee, even if only a traffic offender, might be armed and dangerous. *Id.* at 34-35 & n.5 (citing statistics about officers killed during traffic stops). Allowing the officer some leeway to neutralize the potential danger that an object within an arrestee's reach might contain a weapon or destructible contraband was found reasonable in *Robinson*.

The Court has not interpreted *Robinson* to mean that an arrestee's expectation of privacy in all accompanying effects is necessarily abated. Several years later, in *Chadwick*, *supra*, the Court rejected the government's argument that a warrant requirement should only apply to homes, 433 U.S. at 6-11, and held that a warrant was indeed required to search an arrestee's footlocker. Id. at 13, 15. In rebuffing the government's desire to conduct a warrantless search for evidence on the basis of probable cause, Chief Justice Burger's discussion strongly suggests that the touchstone of when a warrantless search is reasonable is whether it is necessary to ensure an officer's safety or to preserve evidence. *See id.* at 14-15.[8] The Court also recognized in *Arizona v. Gant*, 556 U.S. 332 (2009), that a permissive bright line search incident to arrest rule unmoored from its justifications can be

---

[8] A footnote distinguishing *Robinson* and *United States v. Edwards*, 415 U.S. 800 (1974) (allowing a search of an arrestee's clothing), *id.* at 16 n.10, did not need to explore whether there was or should be any limitation to the permission to search effects found closer to the arrestee's person than the *Chadwick* footlocker.

inappropriately overinclusive, even in the context of vehicular searches, where a lesser expectation of privacy prevails. *See also Thornton v. United States*, 541 U.S. 615, 632 (2004) (Scalia & Ginsburg, JJ, concurring). As Justices Scalia and Ginsburg had observed in *Thornton*, "if carried to its logical end, the broader rule is hard to reconcile with the influential case of *Entick v. Carrington* [citation omitted]." *Id.* at 631,

If *Robinson* is interpreted as giving automatic permission to search the highly sensitive contents of an arrestee's cell phone, it is indeed inconsistent with *Entick*. The point of *Entick* is that the interests surrounding arrest of a person and the interests surrounding the privacy of one's papers and effects, even if they are in the physical vicinity of an arrest, are quite distinct. *See also United States v. Lefkowitz*, 285 U.S. 452, 463-64 (1932) (books and papers in arrestee's office were not subject to search). The fundamental importance of respecting the privacy of personal papers is not reduced by the fact that an officer has probable cause to believe that a cell phone's owner has committed an offense, or that the owner will be in custody.

Given the significance of the privacy interest in the contents of a cell phone and the fact that cell phones ordinarily do not pose any danger -- either to officer safety or to the preservation of evidence -- that cannot be handled by less intrusive means, there is no justification for a *per se* rule exempting a cell phone from the warrant requirement because it is seized incident to arrest. As the Court said in circumscribing the search incident to arrest of a home in *Chimel*, *supra*, "We can see no reason why,

simply because some interference with an individual's privacy and freedom of movement has lawfully taken place, further intrusions should automatically be allowed despite the absence of a warrant that the Fourth Amendment would otherwise require." 395 U.S. at 766-767 n. 12.

History does not teach otherwise. *See* Tracey Maclin, *Annex Perspectives: Cell Phones, Search Incident to Arrest, and the Supreme Court*, 94 B.U.L. Rev. 3 (2014) (neither precedent nor history establishes an unqualified right to search effects); LaFave, *supra*, at § 5.2(c) (accord). In tracing the origins of the search incident to arrest authority it is important to note that in those "simpler times" when the common law was being forged, the targets of that authority were usually felons who had committed violence or stolen property. The purpose of the search incident to arrest was to relieve them of the weapon used or the goods stolen. *See* Telford Taylor, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 28 (1969). This may explain why, as the Court concluded in *Watson* and *Atwater*, the framers were not overly concerned with limiting arrests by local constables and peace officers. But the justification for those common law searches does not extend to a jaywalker bearing a cell phone.

B. A Per Se Rule Prohibiting Cell Phones Searches Absent A Warrant Or Exigent Circumstances Is More Easily Administrable Than Alternative Approaches.

As Chief Justice Burger observed in *Chadwick*, "when no exigency is shown to support the need for an immediate search, the Warrant Clause places the

line at the point where the property to be searched comes under the exclusive dominion of police authority." 433 U.S. at 15. Officers may remove a cell phone from the arrestee, search it immediately if exigent circumstances exist, and seek a search warrant if they have probable cause to search for something in particular. This is an easily administrable rule because it is familiar and because it is grounded in logic – the kind of logic officers regularly employ in deciding whether exigent circumstances exist.

All available alternatives pose problems, both because they are overly permissive and because they cannot be easily and reliably applied by lower courts or officers in the field.

The supposedly bright line *Diaz* rule, *see* 244 P.3d at 509, presents the same questions about degrees of temporal and physical proximity as the now-discarded recent occupant rule of *Thornton*, *supra*. *Diaz* allowed the search of a cell phone ninety minutes after an arrest because, unlike the footlocker in *Chadwick*, it had been on the arrestee's person. 244 P.3d at 505-06. Logically, why should it matter whether a man keeps his cell phone in his pocket, a woman keeps hers in her purse, and another woman in a rolling duffle bag or a footlocker? How long do the police have to search the cell phone of a recent arrestee? *Thornton* posed those same questions, conditioning permission to search an automobile on the temporal and physical proximity of the arrestee and the vehicle, 541 U.S. at 623-24. The Court in *Gant, supra,* replaced that problematic approach with more logical limits: whether an arrestee has access to the object in question at the time of the

proposed search, or whether it is reasonable to believe that evidence of the offense of arrest may be found. *Gant*, 556 U.S. at 335.

Another problem with the *carte blanche* rule of *Diaz* is that once the police are allowed to search a cell phone without a warrant, it is impossible to impose any logical and administrable rule that will set appropriate boundaries to their explorations. The search incident to arrest doctrine dispenses not only with the requirement of a search warrant, but also with the requirement of probable cause. Thus, there is no way to define the scope of the search permitted by applying logic. The proper scope of the search would have to be determined by post-hoc litigation, or by ill-fitting general rules set in advance.

A variety of compromise categorical distinctions have been proposed that would allow some warrantless searches of cell phones incident to arrest and not others, but each has significant drawbacks. *See, e.g.*, Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L. Rev. 183, 209–2 (2010) (examining and rejecting various compromise proposals); Gershowitz, *supra*, at 45-58 (examining six compromise positions and finding all unsatisfying).

Type of Device -- One type of compromise would determine whether a particular device could be searched based on its features, distinguishing, for example, between old-fashioned flip phones and more computer-like smartphones. *See* Orso, *supra*, at 219-22; 223-224. This approach is highly impractical. Technology is evolving so rapidly that a constitutional rule based on today's cell phones will

quickly become outmoded. *Cf. City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010). "Because [even] basic cellphones in today's world have a wide variety of possible functions, it would not be helpful to create a rule that requires officers to discern the capabilities of a cell phone before acting accordingly." *State v. Smith*, 920 N.E.2d at 954. The majority and dissenting judges in *Diaz* agreed that such a line would be impossible for officers in the field to apply, *see* 244 P.3d at 508-09; *id.* at 514 (Werdegar, J., dissenting). *See also United States v. Murphy*, 553 F.3d 405, 411 (4th Cir. 2009).

Type of information seized -- Some suggest that police should be allowed to search any kind of information that has a physical analog, seeing no difference between a digital contacts list and a physical address book.[9] *See, e.g., United States v. Valdez*, No. 06-CR-336, 2008 WL 360548, at 3 (E.D. Wis. Feb. 8, 2008). It was this kind of failure to recognize the distinctive properties of new technology that led the Supreme Court to the infamously

---

[9] It should be noted that this digital analog argument assumes, as some lower courts have, that it is indeed permissible for an officer to read the contents of an arrestee's physical address book without a warrant, *see, e.g., United States v. Holzman*, 871 F.2d 1496, 1504-05 (9th Cir. 1989), rather than confining the scope of a search incident to arrest to what is necessary to protect against danger - like shaking the pages to ensure that no razor blades are present and taking the address book from the arrestee. It can certainly be argued that the permission to search physical effects should never be so broad as to allow the exception to exceed its rationales. *See United States v. Flores-Lopez*, 670 F.3d 803, 805, 807 (7th Cir. 2012); *cf.* LaFave,, *supra*, at § 5.2(c).

mistaken majority decision in *Olmstead v. United States*, 277 U.S. 438 (1928), that the Fourth Amendment does not prohibit warrantless wiretapping of telephones. *Id.* at 465. The voluminous and revealing contents of a cell phone are as far removed from a physical object like a cigarette pack or even a paper address book (either of which might contain a razor blade) as wiretapping is from a constable lurking near a window hoping to overhear a conversation.

Evidence of Offense of Arrest -- Finally, the United States proposes borrowing a standard from *Gant*, 556 U.S. at 343-44, 351, and allowing a cell phone to be searched incident to arrest if there is reason to believe that evidence of the crime of arrest might be found. Brief for Petitioner at 45-49, *United States v. Wurie*, 728 F.3d 1 (1st Cir 2013), *cert. granted*, 134 S.Ct. 999 (2014) (No. 13-212). But this proposal ignores a critical distinction. In *Gant*, the reasonable belief standard was adopted in the context of the search of a vehicle. This Court decided long ago that the search warrant requirement does not apply to vehicles, *see Carroll v. United States*, 267 U.S. 132 (1925). The automobile exception was initially based on the ready mobility of a vehicle as compared to a home, *id.* at 153. The Court has since explained that the exception is also justified by the lesser expectation of privacy in vehicles, first, because they operate in public, and second, because they are subject to pervasive regulation. *See, e.g., South Dakota v. Opperman*, 428 U.S. 364, 368-69 (1976). *Gant* authorized a certain number of evidence-seeking searches incident to arrest of a vehicle in the absence of probable cause, in a context

where a search warrant would not have been required in any event.

This narrow exception should not be carried over to cell phones, whose contents are neither public nor highly regulated. Because the papers and effects in cell phones are so revealing, these devices are far more like the inner sanctum of the home, at the pinnacle of Fourth Amendment protection, than like a vehicle. As *Chadwick* has established, the warrant requirement does apply to at least some effects within an arrestee's possession, 433 U.S. at 11 ("In this case, important Fourth Amendment privacy interests were at stake. . . .There being no exigency, it was unreasonable for the Government to conduct this search without the safeguards a judicial warrant provides."). The *Gant* exception should not be extended to undermine both the warrant and probable cause requirements that, under *Chadwick*, protect our effects as well as our homes.

Furthermore, this seemingly limited exception would be destined to sprawl. There is such a variety of information available within a cell phone that it would often be possible for a creative officer to concoct a connection between the offense of arrest and something potentially somewhere on the phone. After-the-fact litigation would then be necessary to review whether there was a sufficient nexus between the offense of arrest and where the officer searched. And the officer could also be creative in choosing an offense of arrest that would arguably implicate the kind of evidence sought – perhaps an arrest at a demonstration in order to search for evidence of whether the demonstrator and her associates were aware of the permitted parade route, or an arrest for

the offense of "boy dressing as a girl," *see* Walnut City [CA] Code, Title III, Ch 17-31 § 4237.1, *available at* http://qcode.us/codes/walnut/, so the officer could search through photographs for evidence of similar prior conduct. Finally, permitting an officer to search generally for evidence of the offense of arrest without a magistrate's assessment of what in particular may be searched for and where, would raise a host of problems about the proper scope of the search. Additionally, once an officer has begun to search a device looking for one kind of evidence, no matter how defined, questions about what should be regarded as within plain view will be inevitable.[10] Only a *per se* rule, allowing a magistrate to decide the proper scope of a search in an individual case, can offer reasonable and accountable boundaries.

III. CELL PHONES ARE ENTITLED TO HEIGHTENED PROTECTION UNDER THE FOURTH AMENDMENT BECAUSE THEY CONTAIN FIRST AMENDMENT-PROTECTED ASSOCIATIONAL INFORMATION.

Amici agree with petitioner and others that because cell phones contain vast quantities of expressive material, they merit heightened protection from searches incident to arrest. Rather than repeat those arguments, we focus on the additional point that cell phones also deserve

---

[10] "Computer hard drives store a tremendous amount of private information that can be exposed even in a targeted search. If everything comes into plain view, the plain view exception threatens to swallow the rule." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 566 (2005).

heightened protection because they contain substantial quantities of associational materials.

It is well-established that the First Amendment protects the right to associate free from government scrutiny. It is equally clear that searches of First Amendment-protected materials merit heightened protections. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) ("Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'"); *Maryland v. Macon*, 472 U.S. 463, 468 (1985) ("The First Amendment imposes special constraints on searches for and seizures of presumptively protected material").

Traditionally used for coordinating and connecting with friends and family, cell phones are increasingly organizing tools used by political and other associations. Cell phone interconnectivity has evolved from such basic features as contact lists and call displays to a staggering array of interactive features, including social networking applications. A growing proportion of cell phone users send and receive information about political campaigns through their phones. As gateways to larger social networks, cell phones are uniquely conducive to real-time organizing and contingency planning. Police searches through a person's cell phone are likely to reveal the sort of rich associational details that this Court has traditionally forbidden the government from compelling an individual to divulge absent extraordinary circumstances.

A. This Court Has Long Recognized That The First Amendment Protects The Right To Associate In Private.

It is has long been clear that the First Amendment protects against compelled disclosure of one's associations. *NAACP v. Alabama*, 357 U.S. 449, 460 (1958) (recognizing right to be free from compelled disclosure of membership list because "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association.").

The right to associate would be stymied if government could require disclosure of individuals' private associations. *Id.* at 462. "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Id.* Were it otherwise, individuals would feel pressured to "adhere to the most orthodox and uncontroversial views and associations." *Watkins v. United States*, 354 U.S. 178, 197-98 (1957); *see also Shelton v. Tucker*, 364 U.S. 479, 486 (1960).

Moreover, this Court has recognized that forcing a person to disclose his associations to the government not only harms that person, but also inflicts injury on those with whom he chose to associate. *Watkins*, 354 U.S. at 197 ("Nor does the witness alone suffer the consequences. Those who are identified by witnesses and thereby placed in the same glare of publicity are equally subject to public stigma, scorn and obloquy."). This is true even when officials do not abuse their authority by acts of retaliation or public exposure. *Id.* at 197-98.

Just as the right of association protects an organization from having to identify all of its members to government officials, so, too, are individuals protected from efforts to compel disclosure of all of their private associations. *Shelton*, 364 U.S. at 480, 485-86 (striking down statute that required all teachers to identify "every organization to which he has belonged or regularly contributed within the preceding five years" on grounds that "to compel a teacher to disclose his every associational tie is to impair that teacher's right of free association.")

Given the longstanding protections for associational information, the government faces a heavy burden when it curtails associational rights. *Brown v. Socialist Workers '74 Campaign Comm. (Ohio)*, 459 U.S. 87, 91-92 (1982). "The right to privacy in one's political associations and beliefs will yield only to a subordinating interest of the State [that is] compelling, and then only if there is a substantial relation between the information sought and [an] overriding and compelling state interest." *Id.* (alteration in original) (internal quotation marks and citations omitted).

B. Cell Phones Contain A Substantial Amount Of Associational Material.

Given the robust protections for freedom of association, this Court must grapple with the fact that cell phones contain an array of information about a person's associations that is far richer than the disclosures required of teachers in *Shelton*, 364 U.S. at 480-81. Moreover, cell phones play a crucial role in sending and receiving information about political campaigns, and in organizing the very sorts

of public demonstrations and advocacy campaigns that are at the core of the First Amendment's protections.

Cell phones contain substantial quantities of information about our associations because their very purpose is to connect individuals. Contacts lists and call histories, which reveal the identity of an individual's contacts and the frequency of their interactions, as well as text messaging and voicemail, which further disclose the substantive content of a user's communications with associates, are standard features of even basic cell phones.

The advent of internet-enabled "smart phones" has accelerated the development of these standard associational features. A smart phone user can access her associations on social networking sites such as Twitter and Facebook. Through social networking "apps", people engage in quintessential associational activity. They join with others to promote particular viewpoints on pressing questions of the day. They create, distribute and sign petitions. In *Reno v. ACLU*, 521 U.S. 844 (1997), this Court accorded the Internet full First Amendment protection because it recognized the medium's great power to facilitate the speech of ordinary Americans. *Id.* at 870 ("Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."). Particularly after the advent of social networks, the Internet is now a medium through which individuals can engage in the full panoply of associational activities.

Internet users primarily engage in social networking on mobile platforms, so that this type of

associational information is very likely to be on their phones, rather than (or in addition to) their home computers. Vindu Goel, *Big Profit at Facebook as It Tilts to Mobile*, N.Y. Times, Jan. 29, 2014 (three quarters of Facebook's 757 million users log on using mobile devices); Nick Wingfield, *The Numbers Behind Twitter*, N.Y. Times, Oct. 3, 2013 (reporting that three quarters of Twitter's 218.3 million users log on from a mobile device).

The right of association applies to all associations, not just those that are political in nature. *See NAACP v. Alabama*, 357 U.S. at 460 ("[I]t is immaterial whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters."); *NAACP v. Button*, 371 U.S. 415, 430-31 (1963). Critically, however, cell phones play a crucial role in facilitating political engagement.

The evidence suggests that substantial numbers of Americans use their cell phones to send and receive information about political campaigns. Aaron Smith & Maeve Duggan, The State of the 2012 Election—Mobile Politics, Pew Research Center (Oct. 9, 2012), *available at* http://www.pewinternet.org/2012/10/09/the-state-of-the-2012-election-mobile. According to a Pew Research survey of phone usage during the 2012 election, eighty-eight percent of registered voters owned a cell phone, and twenty-seven percent of these "used their phone in this election campaign to keep up with news related to the election itself or to political issues in general." *Id.* Of those in the twenty-seven percent who used text messages, nineteen percent sent campaign-related text messages, and five percent signed up to receive

text messages from a candidate or other group involved in the election. *Id.* Given the rapid adoption of smart phones, political discourse on mobile platforms is the wave of the future.

Of smartphone owners who were surveyed, forty-five percent used their phones to read comments posted by others on social media about the campaign and thirty-five percent used their phone to verify a claim about a candidate or campaign. *Id.*

For the rapidly growing percentage of Americans who use their cell phones to associate with particular candidates and campaigns, then, a police search of these phones entails the substantial risk that the law enforcement agent conducting the search would uncover information about their political associations and beliefs.

For the most politically active and engaged Americans, the risks are even more acute. This is because cell phones have become crucial tools for organizing political demonstrations and promoting other associational activities, as the following examples attest:

- **University of California Tuition Hike Protests.** In November 2009, the University of California regents were set to vote on a 32 percent tuition increase. Students, staff, and faculty mounted major protests in response, including one well-reported demonstration that "was, in part, made possible because students sent last-minute text messages to their friends inviting them to join the march." Bob Samuels, *Facebook, Twitter, YouTube—and Democracy*, 97 Academe (2011).

- **Tea Party Political Campaigns.** American Majority Action, a Tea Party-affiliated, non-profit organization, has invested heavily in a smartphone app that will facilitate more efficient communication between campaign field organizers and their volunteers going door-to-door in neighborhoods. The app, Gravity, allows the volunteers to submit information back to the field organizer about each interaction. Field organizer can then, in real time, change the volunteers' scripts and edit the list of houses to approach. American Majority Action plans to give away the app to local Tea Party groups. Alexander Bolton, *Conservative Group Makes $1M High-Tech Investment to Help Tea Party*, The Hill (Apr. 12, 2012), http://thehill.com/blogs/hillicon-valley/technology/221151-conservative-group-makes-1m-high-tech-investment-to-help-tea-party-groups.

- **Bay Area Rapid Transit (BART) protests.** Activists planned to protest the killing of Charles Blair Hill, who was shot by BART police on July 3, 2011, by coordinating through cell phones. In implicit acknowledgment of the crucial role of cell phones in organizing, BART asked cell phone service providers to halt service in four San Francisco metro stations. In response, activists planned more protests using a Twitter hashtag to communicate. Zusha Elinson, *After Cellphone Action, BART Faces Escalating Protests*, N.Y. Times, Aug. 20, 2011, *available at* http://www.nytimes.com/2011/08/21/us/21bcbart.html?pagewanted=all&_r=2&.

- **Anti-Abortion Organizing and Fundraising.** The Archdiocese of Los Angeles and the non-profit organization Options United have

developed a cell phone app that connects "crisis pregnancy centers," pregnant women and anti-abortion activists. The app, "ProLife," allows any of the 78 crisis pregnancy centers in Southern California to send out "urgent prayer alerts" requesting users to pray for a woman considering an abortion. The app will also send out a "save alert" when a woman decides not to have an abortion. Additionally, the app allows supporters to donate money to the crisis pregnancy centers and invite other people to join the network. LA Archdiocese Launches Pro-Life Networking App, Cath. News Agency (Jan. 23, 2014), http://www.catholicnewsagency.com/news/la-archdiocese-launches-pro-life-networking-app/.

The risk that a person engaged in political activism would be arrested and subject to a search that would reveal substantial information about his private associations is not merely theoretical. A Californian housing rights activist, for example, arrested during a protest of California's anti-lodging law, was occupying the vestibule of his tent when police seized his standard cell phone. Verified Complaint for Injunctive Relief at ¶¶ 16-21, *Offer-Westort v. City & Cnty. of S.F.*, 2013 WL 1149257 (Cal. Super. Mar. 20, 2013) (No. 13-529730). On it, they found organizing communications with other activists and text messages about a City Board of Supervisor who would vote on the anti-lodging bill. *Id.* at ¶¶ 22-32. The identity of other activists in the arrestee's coalition, and their views on the bill and the politician, were all revealed to the police. *Id.* Moreover, the police seized and detained Mr. Offer-Westort's cell phone, chilling his activism and

depriving him of an important tool for organizing activists and lobbying government. *Id.* at ¶¶ 34-38.

* * * * * *

As Justice Robert Jackson once said, expansive power to search incident to arrest is "an easy way to circumvent the protection [the Fourth Amendment] extended to the privacy of individual life." *Harris v. United States*, 331 U.S. 145, 198 (1947) (Jackson, J., dissenting). That circumvention is not justified where the privacy interests at stake are so great, and the actual need to search – except for the purpose of rummaging for evidence among private papers and effects – is so slight.

"[T]he mischief - the threat to liberty and privacy - that led to the inclusion of the Fourth Amendment in the Bill of Rights has not disappeared; it has only changed in form." M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave it Birth*, 85 N.Y.U. L. Rev. 905, 930-31 (2010). The same is equally true for threats to our First Amendment rights. It can be challenging to recognize and address the significance of those changes in form. But, as Justice Louis Brandeis said, in protesting the 1928 decision that failed to come to terms with the unique attributes of the telephone, "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?" *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting). Justice

Brandeis was prescient in asking the question and correct in suggesting that the plain answer is no, that cannot be.

CONCLUSION

The judgment below should be reversed.

Respectfully submitted,

Susan N. Herman
Counsel of Record
250 Joralemon Street
Brooklyn, NY 11201
(718) 780-7945
susan.herman@brooklaw.edu

Steven R. Shapiro
Ezekiel R. Edwards
Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

Linda Lye
American Civil Liberties Union Foundation of Northern California
39 Drumm Street, 2nd Floor
San Francisco, CA 94111

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
MAR 10 2014
OFFICE OF THE CLERK

Nos. 13-132 and 13-212

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari
to the California Court of Appeal, Fourth District
(Additional caption on inside cover)

BRIEF FOR THE AMERICAN LIBRARY ASSOCIATION AND THE INTERNET ARCHIVE AS AMICI CURIAE SUPPORTING RILEY AND WURIE

GRANT P. FONDO
GERALD G. CHACON, JR.
GOODWIN PROCTER LLP
135 Commonwealth Drive
Menlo Park, CA 94025

WILLIAM M. JAY
Counsel of Record
DANIEL ZYTNICK
JOHN C. RAFFETTO
DAVID Y. CHEN
DAVID R. FOX
SHAUNEEN G. WERLINGER
GOODWIN PROCTER LLP
901 New York Ave., N.W.
Washington, DC 20001
wjay@goodwinprocter.com
(202) 346-4000

March 10, 2014

Library of Congress
Law Library

UNITED STATES,

Petitioner,

v.

BRIMA WURIE,

Respondent.

On Writ of Certiorari
to the United States Court of Appeals
for the First Circuit

TABLE OF CONTENTS

Page

INTEREST OF THE AMICI CURIAE 1

SUMMARY OF ARGUMENT 3

ARGUMENT 5

I. A Person's Reading Material Is Quintessentially Private 5

II. Searches Incident To Arrest Do Not Extend To Classically Private Zones Implicating No Risk To Officer Safety Or Evidence Preservation 9

III. Modern Smartphones Store A Trove of Personal Reading Material And Other Private Information That Is Accessible During A Routine Search 13

IV. Police Are Likely To Examine Private Information While Searching A Smartphone 21

A. Law Enforcement Officers Already Seek And Use Electronic Evidence 22

B. Investigators Already Undertake Warrantless Searches of Electronic Devices Whenever Allowed 25

CONCLUSION 26

TABLE OF AUTHORITIES

Page(s)

CASES

Amazon.com LLC v. Lay,
758 F. Supp. 2d 1154 (W.D. Wash. 2010) 6

Arizona v. Gant,
556 U.S. 332 (2009) 11, 12, 13

Barber v. State,
4 So. 3d 9 (Fla. Ct. App. 2009) 24

Board of Ed. v. Pico,
457 U.S. 853 (1982) 5, 6

Chimel v. California,
395 U.S. 752 (1969) 10, 11

City of W. Covina v. Perkins,
525 U.S. 234 (1999) 7

Davidson v. State,
249 S.W.3d 709 (Tex. Ct. App. 2008) 23

Entick v. Carrington,
19 Howell's State Trials 1029 (C.P. 1765) 7

George v. Rehiel,
738 F.3d 562 (9th Cir. 2013) 24

In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.,
706 F. Supp. 2d 11 (D.D.C. 2009) 7

In re Grand Jury Subpoena to Amazon.com Dated August 7, 2006,
246 F.R.D. 570 (W.D. Wis. 2007) 7

Lamont v. Postmaster Gen.,
381 U.S. 301 (1965) 6

Maryland v. Buie,
494 U.S. 325 (1990) 10

McDonald v. United States,
335 U.S. 451 (1948) 9, 10

McIntyre v. Ohio Elections Comm'n,
514 U.S. 334 (1995) 6

New York v. Belton,
453 U.S. 454 (1981) 11

People v. Endacott,
79 Cal. Rptr. 3d 907 (Ct. App. 2008) 25

People v. Mares,
No. A121521, 2010 Cal. App. Unpub. LEXIS
871 (Cal. Ct. App. Feb. 5, 2010) 23

People v. Zirko,
976 N.E.2d 361 (Ill. App. Ct. 2012) 23

Powell v. Schriver,
175 F.3d 107 (2d Cir. 1999) 8

Schmerber v. California,
384 U.S. 757 (1966) 9

Simmons v. State,
912 P.2d 217 (Nev. 1996) 25

Smallwood v. State,
113 So.3d 724 (Fla. 2013) 17

Stanford v. Texas,
379 U.S. 476 (1965) 9

Stanley v. Georgia,
394 U.S. 557 (1969) 4, 6

State v. Cooper,
747 S.E.2d 398 (N.C. Ct. App. 2013) 23

Sterling v. Borough of Minersville,
232 F.3d 190 (3d Cir. 2000) 8

Talley v. California,
362 U.S. 60 (1960) 6

Tattered Cover, Inc. v. City of Thornton,
44 P.3d 1044 (Colo. 2002) 6, 24

United States v. Brown,
374 F. App'x 927 (11th Cir. 2010) 25

United States v. Chadwick,
433 U.S. 1 (1977) 9, 11, 12

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 24

United States v. Flores-Lopez,
670 F.3d 803 (7th Cir. 2012) 17

United States v. Graziano,
558 F. Supp. 2d 304 (E.D.N.Y. 2008) 23

United States v. Kirschenblatt,
16 F.2d 202 (2d Cir. 1926) 11

United States v. Kyle,
No. CR 10-00245-1 JSW, 2011 U.S. Dist.
LEXIS 6791 (N.D. Cal. Jan. 19, 2011) 25

United States v. Robinson,
414 U.S. 218 (1973) 11

United States v. Rumely,
345 U.S. 41 (1953) 6

United States v. Seljan,
547 F.3d 993 (9th Cir. 2008) 24

United States v. Zavala,
541 F.3d 562 (5th Cir. 2008) 18

Weeks v. United States,
232 U.S. 383 (1914) 8

Wilkes v. Wood,
98 Eng. Rep. 489 (1763) 7

STATUTE

18 U.S.C. § 2710 2

OTHER AUTHORITIES

Akhil Reed Amar, *The Fourth Amendment, Boston, and Writs of Assistance*, 30 Suffolk U. L. Rev. 53 (1996) 7

Amazon, *Customize Your Reading on Kindle DX*, http://www.amazon.com/gp/help/customer/display.html?nodeId=200375680 . 15, 16

American Library Ass'n, State Privacy Laws Regarding Library Records, http://www.ala.org/offices/oif/ifgroups/stateifcchairs/stateifcinaction/stateprivacy 2

Android Authority, *Top 5 eBook Reader Apps for Android Phones / Tablets*, http://www.androidauthority.com/top-5-ebook-reader-apps-for-android-phonestablets-44253/ 14

Sebastian Anthony, *There can only be one: Smartphones are the PCs of the future*, ExtremeTech (Aug. 23, 2012), http://www.extremetech.com/computing/134868-there-can-only-be-one-smartphones-are-the-pcs-of-the-future 19

Tim Bajarin, *Why Your Smartphone Will Be Your Next PC*, TIME Tech (Feb. 25, 2013), http://techland.time.com/2013/02/25/why-your-smartphone-will-be-your-next-pc/ 18

John C. Dvorak, *Should We Consider the Smartphone a Computer?*, PCmag.com (Dec. 4, 2012), http://www.pcmag.com/article2/0,2817,2412850,00.asp 18

Peter Eckersley, Seth Schoen, Kevin Bankston, and Derek Slater, *Six Tips to Protect Your Search Privacy*, Electronic Frontier Foundation (Sept. 14, 2006), https://www.eff.org/wp/six-tips-protect-your-search-privacy 20

Federal Bureau of Investigation, U.S. Dep't of Justice, *Digital Evidence Field Guide: What Every Peace Officer Should Know* (1.1 ed. 2007) 23

Eva Galperin, *How to Remove Your Google Search History Before Google's New Privacy Policy Takes Effect*, Electronic Frontier Foundation (Feb. 21, 2012), https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect 20

Barbara A. Genco, *It's Been Geometric! Documenting the Growth and Acceptance of eBooks in America's Urban Public Libraries*, World Library And Information Congress: 75th IFLA General Conference and Council (July 24, 2009) 14

Google Play Books, https://play.google.com/store/apps/details?id=com.google.android.apps.books 14

Doris Small Helfer, *E-Books in Libraries: Some Early Experiences and Reactions*, Searcher (Oct. 1, 2000), http://www.highbeam.com/doc/1G1-66217098.html 14

Mat Honan, *Break Out a Hammer: You'll Never Believe the Data 'Wiped' Smartphones Store*, Wired.com (Apr. 1, 2013, 6:30 AM), http://www.wired.com/gadgetlab/2013/04/smartphone-data-trail/all/ 17, 21

How Many Books Can a Kindle Hold?, http://www.ehow.com/info_12223761_many-books-can-kindle-hold.html 15

How selling on your smartphone leaves you vulnerable to fraud and blackmail: How personal information stored on devices can be easily accessed by new owners, Daily Mail (U.K.), Feb. 6, 2014, http://www.dailymail.co.uk/news/article-2553412/ 21

iBooks, http://www.apple.com/ibooks 14, 16

Internet Archive, *Audio Archive*, https://archive.org/details/audio 16

Internet Archive, *Moving Image Archive*, https://archive.org/details/movies 16

Libraries Connect Communities: Public Library Funding & Technology Access Study 2011-2012, American Libraries (Summer 2012) 14

Mashable, *5 Fantastic Free iPhone E-book Reader Apps* (Apr. 6, 2010), http://mashable.com/2010/04/06/free-iphone-ebook-readers/ 14

Charles E. MacLean, *But Your Honor, A Cell Phone Is Not A Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L. Rev. 37 (2012) 18

Frank McPherson, *Access Your Google Search History On A Smartphone*, Social Times (Aug. 3, 2010, 9:11 PM), https://socialtimes.com/access-your-google-search-history-on-a-smartphone_b47793 20

Bob Minzesheimer, *The changing world of book reading*, USA Today, Oct. 6, 2013, http://www.usatoday.com/story/life/books/2013/10/06/e-books-reading/2877471/ 13

Multnomah County Library, *E-books, streaming media and downloadables*, https://multcolib.org/ebooks-and-downloadables 16

Nat'l Institute of Justice, U.S. Dep't of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* (2d ed. 2008) 22

N.Y. Pub. Library, *Audio & Video Produced by NYPL*, http://www.nypl.org/voices/audio-video 16

Scott Orgera, *How to Manage Your Browsing History In Safari for the iPhone*, http://browsers.about.com/od/allaboutwebbrowsers/ss/iphonehistory.htm 20

Adam Pash, *Your Smartphone Is a Better PC than Your PC Ever Was or Will Be*, Lifehacker.com (Nov. 4, 2010, 9:15 AM), http://lifehacker.com/5681573/your-smartphone-is-a-better-pc-than-your-pc-ever-was-or-will-be 19

Lee Rainie et al., Pew Internet & Am. Life Project, *The rise of e-reading* (Apr. 4, 2012), http://libraries.pewinternet.org/2012/04/04/the-rise-of-e-reading/ 13

Reportbuyer.com, Press Release, *Mobile Data and Applications: State of the Industry, Market Prospects, and Forecast 2013-2018* (Feb. 24, 2014), http://www.marketwatch.com/story/mobile-data-and-applications-state-of-the-industry-market-prospects-and-forecast-2013-2018-2014-02-24 18

Aaron Smith, *Smartphone Ownership 2013*, Pew Research Internet Project (June 5, 2013) http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/ 14

Elizabeth Stawicki, *Smartphones Help Bridge Gaps in Electronic Medical Records*, NPR (Jun. 17, 2013, 4:00 AM), http://www.npr.org/2012/06/17/192596386/smartphones-help-bridge-gaps-in-electronic-medical-records 19

U.S. Secret Service, U.S. Dep't of Homeland Security, *Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders* (3d ed. 2007) 23

WAR AND PEACE, Project Gutenberg, The Internet Archive, https://archive.org/details/warandpeace030164mbp 15

BRIEF FOR THE AMERICAN LIBRARY ASSOCIATION AND THE INTERNET ARCHIVE AS AMICI CURIAE SUPPORTING RILEY AND WURIE

INTEREST OF THE AMICI CURIAE[1]

The American Library Association ("ALA") is a nonprofit professional organization of 57,000 librarians dedicated to providing and improving library services and promoting the public interest in a free and open information society. Founded in 1876, the ALA actively defends the right of library users to read, seek information, and speak freely.

The Internet Archive is a public non-profit organization that was founded to build an "Internet library," with the purpose of offering permanent access for researchers, historians, scholars, and artists to historical collections in digital format. Founded in 1996 and located in San Francisco, California, the Internet Archive collects and receives data and digitizes source material from a multitude of sources, including libraries, educational institutions, government agencies, and private companies. The Internet Archive then provides free access to its data—which include text, audio, moving images, software, TV news, and archived web pages—to researchers, his-

[1] Letters reflecting the parties' consent to the filing of this brief are on file with the Clerk or being lodged herewith. No counsel for a party authored any portion of this brief. No party and no other entity, except *amici*, their members, and their counsel, made any monetary contribution toward the preparation or submission of this brief.

torians, scholars, and the general public throughout the world. As a digital library, the Internet Archive is working to prevent the Internet—a new medium with major historical significance—other "born-digital" materials, and ephemeral physical media from disappearing into the past, by preserving society's cultural artifacts and providing access to them. Collaborating with institutions including the Library of Congress and the Smithsonian, the Internet Archive is working to preserve a record for future generations.

The ALA and Internet Archive submit this brief because open and free access to literature and other writings and media has long been considered essential to education and to the maintenance of an open society. With their expansive digital collections, traditional libraries and the Internet Archive host a variety of digital material that people have a legal right to view without fear that their beliefs, interests, or curiosities will be exposed to government actors.

In the context of bricks-and-mortar libraries, that right of privacy is well established: almost every state has privacy laws requiring libraries to keep user records and reading lists confidential absent a court order.[2] People have an equally important interest in being able to privately view legally permissible material on the Internet—whether that be a political manuscript like *The Communist Manifesto*, religious writings such as the Bible or Quran, or

---

[2] *See* ALA, State Privacy Laws Regarding Library Records, http://www.ala.org/offices/oif/ifgroups/stateifcchairs/stateifcinaction/stateprivacy. Federal law also restricts "video tape services providers" from disclosing information identifying people who request or obtain videos. 18 U.S.C. § 2710.

medical texts discussing treatment for particular diseases or mental illnesses. These and millions of other texts are now available digitally to people with smartphones from numerous sources, including library websites, the Internet Archive, private suppliers of e-books such as Amazon.com, and individual websites. Millions of Americans read books on their phones, which can often hold thousands of books—all of which would be accessible to a law enforcement officer exploring the device. The ALA and the Internet Archive share an interest in protecting readers' right to view this type of material privately, without the risk that law enforcement officers will conduct a suspicionless search of a person's entire electronic library merely because he or she is arrested while carrying a phone.

SUMMARY OF ARGUMENT

Under this Court's precedents, while police could seize a key found in an arrestee's pocket as a search incident to arrest, they could not use that key to enter a home and search the arrestee's personal library. Even carrying out an arrest *in* a home does not license law enforcement to conduct a suspicionless search of every volume in the home library. Today's personal libraries are portable: they can fit on a smartphone, and a smartphone can fit in a pocket in a way that a shelf of books never could. But the contents of those libraries are no less private.

The Constitution affords the strongest possible protection to Americans' right to engage in intellectual inquiry privately and on their own terms. What Americans are reading is ordinarily none of the government's business; this Court has long accepted

"the right to be free from state inquiry into the contents of [one's] library." *Stanley v. Georgia*, 394 U.S. 557, 565 (1969). This case threatens that principle, because it allows police officers to peer into the contents of a person's entire personal library using a device that happens to be found on that person during an arrest.

Given the strong privacy interests implicated by any search of a smartphone, no exception can be justified to the Fourth Amendment's customary requirements for a search of "persons, houses, papers, [or] effects": individualized suspicion and a warrant issued by a neutral magistrate. Smartphones pose no danger to officer safety, and the clumsy expedient of a manual search is hardly necessary to prevent the conscious destruction of evidence. This Court has refused to countenance a search of a locked footlocker incident to arrest. A smartphone provides access to a space more private than any footlocker, and can store many footlockers' worth of private reading material.

Countenancing a suspicionless search like those at issue here will authorize police to use this new investigative technique to gain access to a plethora of private, sensitive information. Police have already shown that they will review private electronic data, ranging from web browsing history to music files, the moment they are allowed to conduct a suspicionless search of a computer. Smartphones are *personal* computers in every sense of the word: if every arrest of a person with a smartphone—a population including more than half the adults in the United States—allows police officers to rummage painstakingly and intrusively through the contents of personal librar-

ies, the loss of constitutionally protected privacy will be great indeed.

ARGUMENT

The Framers held the contents of a person's library sacrosanct—at the very core of the Constitution's protection for the people's "papers and effects." Today a majority of Americans carry in their pockets or pocketbooks the equivalent of an entire library—a library so capacious that for much of our history it would have been impossible to assemble in one place, much less in a pocket. Smartphones are the repository of Americans' private thinking: they contain and record the books we read, the websites we browse, and the conversations we have with friends and intimates. And they retain this recorded data indefinitely. Allowing a police officer making a routine arrest free rein to rummage through massive quantities of private data works a profound intrusion into what the Constitution regards as the most private, most protected sphere of all. None of the considerations underlying the search-incident-to-arrest doctrine can justify giving police that license to rummage. If this Court does not put a stop to it, law enforcement has every incentive to use that investigative technique aggressively.

I. A Person's Reading Material Is Quintessentially Private

"[T]he right to receive ideas is a necessary predicate to the *recipient's* meaningful exercise of his own rights of speech, press, and political freedom." *Board of Ed. v. Pico*, 457 U.S. 853, 867 (1982). Since the Founding, the freedom to read whatever lawful material one chooses has been central not just to the

Constitution, but to the very notion of American self-government: "[A] people who mean to be their own Governors, must arm themselves with the power which knowledge gives." *Id.* (quoting 9 Writings of James Madison 103 (G. Hunt ed. 1910)).

Because "[o]ur whole constitutional heritage rebels at the thought of giving government the power to control men's minds," this Court has long recognized "the right to be free from state inquiry into the contents of [one's] library." *Stanley v. Georgia*, 394 U.S. 557, 565 (1969). The freedom to read necessarily includes the ability to do so without exposing one's reading selections to the government. *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965) (striking down statute that required citizens who wished to receive "communist political propaganda" to reveal their identities before being able to receive these expressive materials); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1052-53 (Colo. 2002) ("[T]he First Amendment embraces the individual's right to . . . read whatever books she wishes to, without fear that the government will take steps to discover which books she buys, reads, or intends to read.").

Government scrutiny of reading choices creates an unacceptable "deterrent effect" on free inquiry. *Lamont*, 381 U.S. at 307; *United States v. Rumely*, 345 U.S. 41, 57-58 (1953) (Douglas, J., concurring) ("When the light of publicity may reach any student, any teacher, inquiry will be discouraged."). Just as the people have a right to speak anonymously, *see, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995); *Talley v. California*, 362 U.S. 60, 64 (1960), they have the corresponding right to receive speech anonymously. *See, e.g., Amazon.com LLC v.*

Lay, 758 F. Supp. 2d 1154, 1167 (W.D. Wash. 2010) ("Citizens are entitled to receive information and ideas through books, films, and other expressive materials anonymously."); *In re Grand Jury Subpoena to Amazon.com Dated August 7, 2006*, 246 F.R.D. 570, 572 (W.D. Wis. 2007) (holding that government could not obtain identities of people who bought books because "customers who bought used books from [seller] through Amazon do have a cognizable First Amendment right"); *see also In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 17, 21 (D.D.C. 2009) (denying motion to compel production of information on customers who purchased movies; "the expressive materials being investigated are presumptively protected by the First Amendment and [the company's] customers have a correlative right to receive that information anonymously").

Reading choices thus are at the heart of the personal privacy that the Fourth Amendment guarantees. The Fourth Amendment was drafted, in part, as a response to officers of the King who, acting pursuant to general warrants, searched citizens' book collections. *See Wilkes v. Wood*, 98 Eng. Rep. 489 (1763) (several of the King's officers seized all of Wilkes's books and papers with the intent of finding anti-government pamphlets); *Entick v. Carrington*, 19 Howell's State Trials 1029 (C.P. 1765) (officers entered Entick's home and seized his personal "books and papers" in their search for "very seditious papers"). Those "celebrated cases . . . profoundly influenced the Founders' view of what a 'reasonable' search entailed." *City of W. Covina v. Perkins*, 525 U.S. 234, 247 (1999) (Thomas, J., concurring); *see also* Akhil Reed Amar, *The Fourth Amendment, Bos-*

ton, and Writs of Assistance, 30 Suffolk U. L. Rev. 53, 77 (1996) (noting that the words of the Fourth Amendment "seem to track *Wilkes* and *Entick*").

The constitutional protection of private correspondence is well established, *see, e.g.*, *Weeks v. United States*, 232 U.S. 383, 393 (1914), and private reading material is, if anything, more personal and more intimate in nature: a person may read a book, a political pamphlet, or a website in complete solitude, and complete privacy. Indeed, some reading choices—including many offered by *amici* in their traditional and electronic libraries—call for the utmost privacy protection. People may read to explore controversial ideas, such as those contained in the *Communist Manifesto* or *Mein Kampf*. Or they may read to better understand themselves, including aspects of human sexuality that are deeply personal and private. *Cf., e.g.*, *Sterling v. Borough of Minersville*, 232 F.3d 190, 196 (3d Cir. 2000) (holding that "[plaintiff's] sexual orientation was an intimate aspect of his personality entitled to privacy protection"); *Powell v. Schriver*, 175 F.3d 107, 111 (2d Cir. 1999) (concluding that "the Constitution does indeed protect the right to maintain the confidentiality of one's transsexualism"). Whatever the reason, the choice remains the individual's to make, free from the government's gaze. That expectation of privacy is not just "reasonable," in Fourth Amendment parlance, but essential.

II. Searches Incident To Arrest Do Not Extend To Classically Private Zones Implicating No Risk To Officer Safety Or Evidence Preservation

The federal and state governments in these cases submit that a lawful arrest grants the police access to *anything* on the arrestee's person, no matter how grave the intrusion on privacy rights or how attenuated the connection to the arrest. The search-incident-to-arrest doctrine does not extend so far. As this Court has repeatedly held, an arrest is not an unlimited license to search. Rather, the search-incident-to-arrest doctrine takes account of, and is limited by, "Fourth Amendment values" of personal privacy. *United States v. Chadwick*, 433 U.S. 1, 13 n.8 (1977). Nothing in this Court's cases requires it to overlook the drastic loss of personal privacy that permitting suspicionless searches of smartphones would create. A smartphone functioning as an e-reader is a powerful, portable tool not just of communication, but of free inquiry. Protecting that tool against arbitrary search serves the Fourth Amendment's role "safeguarding not only privacy . . . but conscience and human dignity and freedom of expression as well." *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (citation and internal quotation marks omitted).

The Fourth Amendment "protect[s] personal privacy and dignity against unwarranted intrusion by the State." *Schmerber v. California*, 384 U.S. 757, 767 (1966); *see also McDonald v. United States*, 335 U.S. 451, 453 (1948) ("[The Fourth Amendment] marks the right of privacy as one of the unique values of our civilization . . . ."). The warrant require-

ment is a key safeguard of those privacy rights. *McDonald*, 335 U.S. at 455-56 ("The presence of a search warrant serves a high function. . . . It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals.").

Searches presumptively require a warrant; searches without a warrant are exceptions to the norm. The government's authority to conduct a warrantless search incident to arrest, therefore, "has always been considered to be a strictly limited right." *Chimel v. California*, 395 U.S. 752, 759 (1969). The limitation reflects the importance of privacy rights. For a search to be permissible, the government's legitimate justification must outweigh the "intrusion on the individual's Fourth Amendment interests." *Maryland v. Buie*, 494 U.S. 325, 331 (1990). Privacy interests thus help the Court define the boundary between a permissible and impermissible search incident to arrest.

"[S]imply because" a person has been arrested, and thus "some interference with [his] privacy and freedom of movement has lawfully taken place," does not mean that "further intrusions should automatically be allowed." *Chimel*, 395 U.S. at 766 n.12. Rather, this Court has examined "the invasion of privacy that results" from a search incident to arrest, and whether that invasion is sufficiently justified to be reasonable "despite the absence of a warrant that the Fourth Amendment would otherwise require." *Id.*

Governmental interests related to "officer safety and evidence preservation," *Arizona v. Gant*, 556 U.S. 332, 337 (2009), can justify some searches incident to arrest. *See United States v. Robinson*, 414 U.S. 218, 234 (1973) (discussing the "justification or reason for the authority to search incident to a lawful arrest"); *New York v. Belton*, 453 U.S. 454, 461 (1981) (lawful arrest "justifies the infringement" of arrestee's privacy interest). But those interests must be balanced against the personal privacy interest at the core of the Fourth Amendment. *Gant*, 556 U.S. at 335.

Thus, for instance, the Court refused to countenance a search of an entire home incident to an arrest. *Chimel*, 395 U.S. at 767-68. The search created an additional "intrusion" on personal privacy, the Court explained, and not a "minor" one. *Id.* at 766 n.12. It was acceptable to search an arrestee's "person and the area 'within his immediate control,'" but there was no "comparable justification" for searching in other rooms in the arrestee's house or "for searching through all the desk drawers or other closed or concealed areas in that room [where the arrest occurred]." *Id.* at 763. Private papers are supposed to remain private whether or not they are in the same house as an arrestee. *See id.* at 767-68. So too here: "it is small consolation to know that one's papers are safe only so long as one [does not carry them]." *Id.* at 768 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (L. Hand, J.)).

Similarly, the Court refused to allow a search incident to an arrest to extend to a locked footlocker. *Chadwick*, 433 U.S. at 14-16 & n.10. Luggage is "not

open to public view"; its contents are kept private, and for that reason government agents could not open the footlocker until they could get a warrant. *Id.* at 14. The defendants' "privacy interest in the contents of the footlocker was not eliminated simply because they were under arrest." *Id.* at 16 n.10. So too with the passenger compartment of a car, not to mention "every purse, briefcase, or other container within that space." *Gant*, 556 U.S. at 345.

The federal government submits that those decisions are distinguishable because they involved searches *beyond the person* incident to arrest. *E.g.*, U.S. Br. 13, 21-23. That arbitrary distinction (which apparently would treat "persons" differently from "papers and effects") is one without any real difference. But even if it made sense to declare an arrestee's "person" subject to fewer limitations, that rationale would not apply to the contents of a phone in the arrestee's pocket. As discussed below, a smartphone is far more than a physical object; it is a tool for storing, searching, and viewing incredible amounts of data. It is a sizeable chunk of the arrestee's personal papers, reduced to electrons and "not open to public view." It can carry more books than Chadwick's locked footlocker could. It stands to reason that it should receive equivalent protection.

Allowing the search-incident-to-arrest doctrine to override the privacy interest in access to a smartphone would impair the "central concern underlying the Fourth Amendment"—namely, "the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." *Gant*, 556 U.S. at 345. To allow a search in that cir-

cumstance "creates a serious and recurring threat to the privacy of countless individuals." *Id.*

III. Modern Smartphones Store A Trove of Personal Reading Material And Other Private Information That Is Accessible During A Routine Search

If a person were arrested while carrying a key to his personal library of 6000 books, including his highlights in the books and notes relating to the books, there would be no constitutional basis to search those books incident to arrest. Yet by permitting a police officer to search today's smartphone upon arrest, that is exactly what this Court would be permitting. A smartphone is a portal to a person's entire electronic library; in fact, for millions of Americans, it *is* their primary library. Searching a smartphone would give the officer access to many times more books than an arrestee could ever carry in his pocket. And because of the way smartphones work, they often contain not just what the arrestee is reading *today*, but also what he read yesterday, and perhaps years ago—his entire reading history. The mere fact of an arrest does not justify allowing law enforcement to rummage through that massive quantity of often deeply personal data.

Using smartphones, tablets, and dedicated e-readers, millions of Americans now do some or all of their reading on small, portable electronic devices—and the numbers are rapidly increasing.[3] Numerous

---

[3] Lee Rainie et al., Pew Internet & Am. Life Project, *The rise of e-reading* (Apr. 4, 2012), http://libraries.pewinternet.org/2012/04/04/the-rise-of-e-reading/ (21% of American adults read an e-book in the past year); Bob Minzesheimer, *The changing world*

programs—known as apps—allow people to read e-books on their smartphones.[4]

Millions of e-books are available for people to download onto their smartphones.[5] People can also borrow e-books: traditional public libraries started lending e-books in the 1990s,[6] and the numbers have greatly increased since then as libraries make digital books (and often e-readers themselves) available to borrowers.[7]

---

of book reading, USA Today, Oct. 6, 2013, http://www.usatoday.com/story/life/books/2013/10/06/e-books-reading/2877471/ (noting two- and three-fold increases in e-reader and tablet ownership between 2011 and 2013); *see also* Aaron Smith, Pew Research Internet Project, *Smartphone Ownership 2013* (June 5, 2013) http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/ (percentage of American adults who own a smartphone has increased from 35% in 2011 to 56% in 2013).

[4] *See, e.g.*, Android Authority, *Top 5 eBook Reader Apps for Android Phones/Tablets*, http://www.androidauthority.com/top-5-ebook-reader-apps-for-android-phonestablets-44253/; Mashable, *5 Fantastic Free iPhone E-book Reader Apps* (Apr. 6, 2010), http://mashable.com/2010/04/06/free-iphone-ebook-readers/.

[5] iBooks, http://www.apple.com/ibooks (over 2 million books at the iBooks Store, many of them free); Google Play Books, https://play.google.com/store/apps/details?id=com.google.android.apps.books ("Choose from millions of books," which can be read on Android smartphones).

[6] Doris Small Helfer, *E-Books in Libraries: Some Early Experiences and Reactions*, Searcher (Oct. 1, 2000), http://www.highbeam.com/doc/1G1-66217098.html.

[7] Barbara A. Genco, *It's Been Geometric! Documenting the Growth and Acceptance of eBooks in America's Urban Public Libraries*, World Library And Information Congress: 75th IFLA General Conference and Council (July 24, 2009); *Libraries Connect Communities: Public Library Funding & Technology Access*

The growing use of smartphones to read e-books means that the mere fact of an arrest threatens to expose to government agents wide-ranging aspects of people's reading habits—including what books they read, what parts of books they thought interesting or intellectually provocative, what thoughts they had about books. Smartphones now have 64 gigabytes of storage space, enough to fit more than 50,000 copies of War and Peace, so a person's entire library can be accessible with a few clicks using a tiny device.[8] Equally problematic is that readers' interaction with their books is also easy for police officers to see: e-books allow users to take notes, highlight text, or clip what they read.[9] Thus, an officer thumbing through a person's smartphone would see not only the person's books, but what passages the reader thought were compelling or important and what notes the reader took.

The technology works seamlessly across devices, so a person's reading habits (as well as those of a

---

Study 2011-2012, American Libraries (Summer 2012) Digital Supplement at 6 (as of 2012, over 76 percent of libraries offer access to e-books, and 39 percent allow patrons to borrow e-book readers).

[8] *See* WAR AND PEACE, Project Gutenberg, The Internet Archive, https://archive.org/details/warandpeace030164mbp (file size for "epub" version); *see also How Many Books Can a Kindle Hold?*, http://www.ehow.com/info_12223761_many-books-can-kindle-hold.html (estimating that an 8 gigabyte e-reader introduced in March 2012 can store about 6,000 books).

[9] Amazon, *Customize Your Reading on Kindle DX*, http://www.amazon.com/gp/help/customer/display.html?nodeId=200375680 (Amazon, *Customize Your Reading*) ("Kindle allows you to add comments, make notes, and mark up passages just as you might in a printed book.")

spouse or child) may be exposed even if no one was reading the book on the seized smartphone.[10] Reading can be synchronized across devices, including across a family's shared devices, so someone who read part of a book at home on a tablet computer can continue reading on a smartphone or note text for a family member to read—but so could an officer who, upon searching the phone, would be able to see what the person read at home, as well as highlights and notes the person took.[11]

The officer searching the phone could do the same with the user's audio and video files, which are growing in popularity as alternative, smartphone-friendly ways to consume intellectual content. The Internet Archive and other libraries offer numerous forms of audio and video content that can reside on smartphones, including audiobooks, radio programs, podcasts, music, documentaries, and other films.[12]

---

[10] iBooks, http://www.apple.com/ibooks ("[Y]ou can read one of your favorites on your iPhone during your morning commute, page through a few chapters on your Mac later in the day, and pick up right where you left off on your iPad at bedtime.").

[11] iBooks, http://www.apple.com/ibooks ("When you take notes, highlight passages, or create bookmarks, iCloud pushes them to all your devices automatically. And it remembers which page you're on, so you can pick up right where you left off."); Amazon, *Customize Your Reading* ("When you open the title on any registered device, you'll be right where you were the last time you read and your annotations will be included.").

[12] *See, e.g.*, Internet Archive, *Audio Archive*, https://archive.org/details/audio; Internet Archive, *Moving Image Archive*, https://archive.org/details/movies;, N.Y. Pub. Library, *Audio & Video Produced by NYPL*, http://www.nypl.org/voices/audio-video; Multnomah County Library, *E-books, streaming media and downloadables*, https://multcolib.org/ebooks-and-downloadables (providing service that "enables li-

Audiobooks, Internet radio, podcasts, and other multimedia sources are entitled to the same protection for private intellectual inquiry as words on the printed page: they often allow people to see and hear different perspectives, explore controversial ideas, and learn new information, using a medium far more friendly to instant, widespread dissemination than the printing of a traditional book.

A person's expansive digital library is one of the many private things that might be stored on a smartphone, which contributes to the sentiment that "[f]ew things are more precious, intimate and personal than the data on your smartphone."[13] "Vast amounts of private, personal information can be stored and accessed in or through these small electronic devices." *Smallwood v. State*, 113 So.3d 724, 731-32 (Fla. 2013). Smartphones are thus not much different from personal computers in terms of the types of information that they possess. *United States v. Flores-Lopez*, 670 F.3d 803, 805 (7th Cir. 2012) ("Judges are becoming aware that a computer (and remember that a modern cell phone is a computer) is not just another purse or address book. . . . computers hold so much personal and sensitive information

---

brary patrons to watch and listen to a wide selection of movies, television shows, educational and instructional videos, documentaries and music through a browser, smartphone or tablet").

[13] Mat Honan, *Break Out a Hammer: You'll Never Believe the Data 'Wiped' Smartphones Store*, Wired.com (Apr. 1, 2013, 6:30 AM), http://www.wired.com/gadgetlab/2013/04/smartphone-data-trail/all/ ("It tracks your location and logs your calls. It's your camera and your mobile banking device; in some cases it is a payment system in and of itself that knows what you bought and when and where and for how much.").

touching on many private aspects of life."); *United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008) ("[C]ell phones contain a wealth of private information, including emails, text messages, call histories . . . A cell phone is similar to a personal computer that is carried on one's person").[14] Indeed, the pure volume of information that a smartphone can store is remarkable, and rivals that of computers.[15] Moreover, with the convenience that a phone affords, and the exponential growth and increasing utility of downloadable applications,[16] individuals may want

---

[14] Tim Bajarin, *Why Your Smartphone Will Be Your Next PC*, TIME Tech (Feb. 25, 2013), http://techland.time.com/2013/02/25/why-your-smartphone-will-be-your-next-pc/ ("The basic idea here is that the smartphone itself is your PC and then docks into the back of either a portable screen or some type of laptop shell . . . Keep in mind that the smartphone has all of your personal data, personal user interface and personal apps"); John C. Dvorak, *Should We Consider the Smartphone a Computer?*, PCmag.com (Dec. 4, 2012), http://www.pcmag.com/article2/0,2817,2412850,00.asp ("I think the argument can be made that the smartphone is in the same market as the desktop computer").

[15] Charles E. MacLean, *But Your Honor, A Cell Phone Is Not A Cigarette Pack: An Immodest Call For A Return To The Chimel Justifications For Cell Phone Memory Searches Incident To Lawful Arrest*, 6 Fed Cts. L. Rev. 37, 42 (2012) ("A cell phone with just one gigabyte of memory can store over 64,000 pages of Microsoft Word text, or over 100,000 pages of e-mails, or over 675,000 pages of text files. . . . modern cell phones are capable of storing at least sixty-four gigabytes of private information equaling four million pages of Microsoft Word documents").

[16] Reportbuyer.com, Press Release, *Mobile Data and Applications: State of the Industry, Market Prospects, and Forecast 2013-2018* (Feb. 24, 2014), http://www.marketwatch.com/story/mobile-data-and-applications-state-of-the-industry-market-prospects-and-forecast-2013-2018-2014-02-24 ("Mobile applications continue an explosive growth phase. . . . Mobile apps are

to put more private information on their smartphone than even on their home computer.[17]

In many ways, storing and consuming media on a smartphone offers increased privacy for users over physical media. Unlike hardcopy books, records, tapes, CDs, or DVDs, digital books, audio, and video on a smartphone need not be hidden when a person has visitors. And digital media, especially e-books, can be experienced in a crowded public setting with-

---

more than just a direct to consumer phenomenon as leading enterprise companies take mobile apps seriously. . . . [T]oday leading companies are focused on compelling mobile apps."); *see, e.g.*, Elizabeth Stawicki, *Smartphones Help Bridge Gaps in Electronic Medical Records*, NPR (Jun. 17, 2013, 4:00 AM), http://www.npr.org/2012/06/17/192596386/smartphones-help-bridge-gaps-in-electronic-medical-records ("Hospitals, doctors and Medicare are making it easier for people to have access to their own health records. Some [mobile] app developers have even created ways to have health information available even on a smartphone.")

[17] *See* Adam Pash, *Your Smartphone Is a Better PC than Your PC Ever Was or Will Be*, Lifehacker.com (Nov. 4, 2010, 9:15 AM), http://lifehacker.com/5681573/your-smartphone-is-a-better-pc-than-your-pc-ever-was-or-will-be ("Smartphones are PCs . . . only they're more personal . . what's more personal than a gadget that . . . comes with you wherever you go, knows where you are, is always connected to the internet, handles every form of electronic communication short of Morse code . . . And so on."); Sebastian Anthony, *There can only be one: Smartphones are the PCs of the future*, ExtremeTech (Aug. 23, 2012), http://www.extremetech.com/computing/134868-there-can-only-be-one-smartphones-are-the-pcs-of-the-future ("In a few years, everything you do on your laptop today will be achievable on a smartphone. So why continue to use a laptop? . . . In a world where smartphones rule supreme, and extra connectivity is provided by docking stations, there really is no hope for the PC. If it helps, you can simply think of a smartphone as a really small PC.").

out drawing the attention of snoops. In these ways, a person's digital library is more private than a physical library in his or her home.

The extraordinary capabilities of modern smartphones encourage users to expose every facet of their lives to their devices. With the enhanced productivity and connectedness comes increased risk: if the information stored on the individual's phone may be accessed by a police officer incident to every arrest, the privacy interests of individuals will be severely compromised. Virtually every single activity on a smartphone is logged and stored. Someone looking at a smartphone can see a person's text messages, emails, and internet search and browsing history.[18] Just as books read at home can show up on a smartphone, searches that a person runs from a home computer may show up in the search history on his or her phone.[19] Even more alarming, regardless of

---

[18] *See, e.g.*, Eva Galperin, *How to Remove Your Google Search History Before Google's New Privacy Policy Takes Effect*, Electronic Frontier Foundation (Feb. 21, 2012), https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect; Peter Eckersley, Seth Schoen, Kevin Bankston, and Derek Slater, *Six Tips to Protect Your Search Privacy*, Electronic Frontier Foundation (Sept. 14, 2006), https://www.eff.org/wp/six-tips-protect-your-search-privacy ("Google, MSN Search, Yahoo!, AOL, and most other search engines collect and store records of your search queries."); Scott Orgera, *How to Manage Your Browsing History in Safari for the iPhone*, http://browsers.about.com/od/allaboutwebbrowsers/ss/iphonehistory.htm ("The Safari Web browser on your iPhone keeps a log of Web pages that you have visited in the past.").

[19] Frank McPherson, *Access Your Google Search History On A Smartphone*, Social Times (Aug. 3, 2010, 9:11 PM), https://socialtimes.com/access-your-google-search-history-on-a-

whether an individual wants to record the information or even knows that the information is being stored, more likely than not, that information can be found by someone who gains access to the individual's phone.[20] Digital books are just one important example among the numerous categories of personal material that can easily be exposed.

IV. Police Are Likely To Examine Private Information While Searching A Smartphone

If this Court approves the routine search of smartphones incident to arrest, the privacy impact will be immediate and dramatic. That is not a prediction; it is a certainty. Evidence of the sort available on smartphones is commonly used by the gov-

---

smartphone_b47793 ("If you have a Google account, and sign in to it from a web browser, then all of the searches that you perform in Goggle are stored by Google.").

[20] For example, even after a modern cell phone (albeit not the newest version) was disposed of, and its personal data mostly deleted, a mobile forensics expert was able to find hundreds of phone numbers from a contacts database and "a list of nearly every Wi-Fi and cellular access point the phone had ever come across – 68,390 Wi-Fi points and 61,202 cell sites. . . . Even if the phone had never connected to any of the Wi-Fi access points, iOS was still logging them, and [the forensics expert] was able to grab them and piece together a trail of where the phone had been turned on." Honan, *supra*; *see also How selling on your smartphone leaves you vulnerable to fraud and blackmail: How personal information stored on devices can be easily accessed by new owners*, Daily Mail (U.K.), Feb. 6, 2014, http://www.dailymail.co.uk/news/article-2553412 (reporting that "[p]hotos, passwords and credit cards are just some of the intimate details" that smartphone owners "unwittingly" store on their devices, and "can be easily accessed").

ernment in criminal cases of all kinds, and investigators already undertake frequent warrantless searches of electronic devices where courts have allowed it,.

A. Law Enforcement Officers Already Seek And Use Electronic Evidence

Law enforcement officers are trained to view electronic devices as a potent source of potential evidence. If permitted, they will fully exploit any authorization to search smartphones without individualized suspicion or a warrant.

Reference materials for first responders advise them to be zealous in collecting electronic devices, including smartphones, as evidence. In a 2008 guide for "First Responders," the Justice Department's National Institute of Justice advised that "handheld devices such as mobile phones [and] smart phones . . . may contain software applications, data, and information such as documents, e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, and financial records that are valuable evidence in an investigation or prosecution." Nat'l Institute of Justice, U.S. Dep't of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* 8 (2d ed. 2008). When securing a scene, first responders are advised to "[i]mmediately secure *all* electronic devices, including personal or portable devices." *Id.* at 15. And mobile devices are listed as "potentially valuable digital evidence" for every category of crime addressed by the guide. *Id.* at 35-46.

The Secret Service and the Federal Bureau of Investigation have similarly advised first responders of the value of smartphone evidence for investigations

of all sorts. *See* U.S. Secret Service, U.S. Dep't of Homeland Security, *Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders* 6, 12-14 (3d ed. 2007); Federal Bureau of Investigation, U.S. Dep't of Justice, *Digital Evidence Field Guide: What Every Peace Officer Should Know* 4-6 (1.1 ed. 2007).

Further driving investigators to search electronic devices, a growing number of criminal cases have involved the sort of evidence available on smartphones. In a 2010 California case, the jury was told that the defendant had "viewed the Military Library portion" of a website, "which involved silencers, body armor, explosives, and the like" and which "listed several books about silencers." *People v. Mares*, No. A121521, 2010 Cal. App. Unpub. LEXIS 871, at *9-10 (Cal. Ct. App. Feb. 5, 2010). The *Mares* jury also learned that the defendant had visited a website about videos depicting various forms of extreme violence—violence entirely unrelated to the crime at issue. *Id.* Other evidence of internet search results has also been used in prosecutions. *See Davidson v. State*, 249 S.W.3d 709, 716 (Tex. Ct. App. 2008) (jury learned that the defendant had conducted an internet search for "decomposition of a body in water"); *United States v. Graziano*, 558 F. Supp. 2d 304, 314-15 (E.D.N.Y. 2008) (investigators found internet search for "arson rico laws"). So has evidence about what people looked at on online maps. *See People v. Zirko*, 976 N.E.2d 361, 373 (Ill. App. Ct. 2012) (defendant searched MapQuest.com for directions to the crime scene); *State v. Cooper*, 747 S.E.2d 398, 402 (N.C. Ct. App. 2013) (defendant used Google Maps to "zoom[] in on the exact spot" where the victim's body was later found). And the jury in a Florida case

learned about a song that the defendant downloaded on the day that his wife was killed. *Barber v. State*, 4 So. 3d 9, 10-11 (Fla. Ct. App. 2009) (the Guns N' Roses song "Used to Love Her (But I Had to Kill Her)").[21]

As an increasing number of people read books on their smartphones, law enforcement officers are likely to examine this information to see what books arrestees have been reading to gain evidence of criminal activity. Police already do that with printed books. *See George v. Rehiel*, 738 F.3d 562, 586 (9th Cir. 2013) (college student detained by Transportation Security Administration and questioned about Arabic flash-cards and a book "critical of United States foreign policy" from his luggage); *United States v. Seljan*, 547 F.3d 993, 998 (9th Cir. 2008) (en banc) (police seized a "fiction book about pedophilia and incest" in connection with a sex-crimes prosecution); *Tattered Cover*, 44 P.3d at 1061 (law-enforcent officials served bookstore with an administrative subpoena demanding to know every book a particular suspect had ever ordered); *Simmons v. State*, 912 P.2d 217, 220 (Nev. 1996) (police seized a book about Satanism and read portions of it at defendant's murder trial). For every example in a reported opinion,

---

[21] Other cases—particularly child-pornography cases—involve electronic material that is itself contraband. *See, e.g., United States v. Cotterman*, 709 F.3d 952, 957-58 (9th Cir. 2013). *Amici* do not host contraband, but officers searching for it might well come across private and personal material of the sort that *amici* do host. And the possibility of discovering such contraband gives investigators another reason to search electronic devices eagerly, and thereby increases the chance that investigators will discover the sort of "research" evidence discussed above that does implicate *amici*'s interests.

it is likely that there are far more instances in which police rummaging through someone's reading material find no useful evidence—but the infringement on privacy has already occurred.

B. Investigators Already Undertake Warrantless Searches of Electronic Devices Whenever Allowed

Law enforcement officers are entirely capable of finding private and personal information on electronic devices. In *United States v. Brown*, for example, a detective executing a warrant saw a computer and quickly "look[ed] at the search history for Google, the site to which it was opened." 374 F. App'x 927, 937 (11th Cir. 2010). Similarly, Customs officers often examine files on electronic devices. *See People v. Endacott*, 79 Cal. Rptr. 3d 907, 908 (Ct. App. 2008) (Customs officer regularly powers up laptops and looks for pictures and video); *United States v. Kyle*, No. CR 10-00245-1 JSW, 2011 U.S. Dist. LEXIS 6791, at *2-3 (N.D. Cal. Jan. 19, 2011) (customs officer conducted "a media examination" of cell phone and laptop).

Given the extraordinary growth in the use of smartphones and correspondingly increasing role of electronic evidence, the Court can expect an explosion of warrantless smartphone searches if it upholds them here—such searches will be standard operating procedure. And the increase would reflect searches that, under the law in force today, cannot be conducted without individualized suspicion and a warrant. Investigators hoping to find evidence of the sort identified above already exploit any opportunity to search electronic devices. As discussed above, the

wealth of information available on a smartphone makes those devices much like a modern computer, but more personal, because people carry the devices with them everywhere they go. As a result, while many of the cases discussed above involved warrants, investigators also take advantage of exceptions to the warrant requirement to conduct warrantless searches of electronic devices wherever courts have permitted them.

If this Court announces a rule allowing a suspicionless search of every cell phone that is found on an arrestee's person, law enforcement will not pass up the opportunity. The result will be precisely the sort of suspicionless "rummaging" that this Court's cases forbid, and the impact on privacy will be severe.

CONCLUSION

The judgment in *Riley* should be reversed, and the judgment in *Wurie* should be affirmed.

Respectfully submitted.

GRANT P. FONDO
GERALD G. CHACON, JR.
GOODWIN PROCTER LLP
135 Commonwealth Drive
Menlo Park, CA 94025

WILLIAM M. JAY
Counsel of Record
DANIEL ZYTNICK
JOHN C. RAFFETTO
DAVID Y. CHEN
DAVID R. FOX
SHAUNEEN G. WERLINGER
GOODWIN PROCTER LLP
901 New York Ave., N.W.
Washington, DC 20001
wjay@goodwinprocter.com
(202) 346-4000

March 10, 2014

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
APR - 9 2014
OFFICE OF THE CLERK

No. 13-132

In the Supreme Court of the United States

REPRINTED COPY

DAVID LEON RILEY,
Petitioner,

v.

STATE OF CALIFORNIA,
Respondent.

On Writ of Certiorari to the Court of Appeal of California, Fourth Appellate District, Division One

BRIEF OF THE STATES OF ARIZONA, ET AL., AS *AMICI CURIAE* SUPPORTING RESPONDENT

THOMAS C. HORNE
Arizona Attorney General
ROBERT L. ELLMAN
Solicitor General
JOSEPH T. MAZIARZ
Chief Counsel, Criminal Appeals Section
MICHAEL T. O'TOOLE
Assistant Attorney General
Counsel of Record
1275 West Washington Street
Phoenix, AZ 85007
Phone (602) 542-8551
Fax (602) 542-4849
michael.otoole@azag.gov
Counsel for Amici Curiae

(additional counsel listed on inside cover)

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

Library of Congress
Law Library

JOHN W. SUTHERS
Attorney General
State of Colorado

JOSEPH R. BIDEN, III
Attorney General
State of Delaware

DAVID M. LOUIE
Attorney General
State of Hawaii

LAWRENCE G. WASDEN
Attorney General
State of Idaho

JAMES D. CALDWELL
Attorney General
State of Louisiana

JIM HOOD
Attorney General
State of Mississippi

CATHERINE CORTEZ MASTO
Attorney General
State of Nevada

GARY K. KING
Attorney General
State of New Mexico

WAYNE STENEHJEM
Attorney General
State of North Dakota

ALAN WILSON
Attorney General
State of South Carolina

MARTY J. JACKLEY
Attorney General
State of South Dakota

ROBERT E. COOPER, JR.
Attorney General
State of Tennessee

J.B. VAN HOLLEN
Attorney General
State of Wisconsin

PETER K. MICHAEL
Attorney General
State of Wyoming

QUESTION PRESENTED

Whether the Fourth Amendment prohibits a police officer from searching a cell phone as part of a search incident to an arrest.

TABLE OF CONTENTS

PAGE

QUESTION PRESENTED i

TABLE OF AUTHORITIES iii

INTEREST OF AMICI CURIAE 1

SUMMARY OF THE ARGUMENT .. 1

ARGUMENT 3

A. The Policies Furthered by the Broad Search-Incident-to-Arrest Exception Apply to the Contents of a Cell Phone. 3

B. No Principled Basis Exists to Exclude the Search of a Cell Phone from the Search-Incident-to-Arrest Exception. 7

C. Law Enforcement Officers Need Clear Workable Rules, Like the One Articulated in *Robinson*. 12

CONCLUSION 15

TABLE OF AUTHORITIES

CASES **PAGE**

Agnello v. United States,
269 U.S. 20 (1925) 7

Arizona v. Gant,
556 U.S. 332 (2009) 4

Chimel v. California,
395 U.S. 752 (1969) 4

Dunaway v. New York,
442 U.S. 200 (1979) 13

Farrington v. Smith,
707 F.3d 963 (8th Cir. 2013) 10

Fawdry v. State,
70 So.3d 626 (Fla. App. 2011) 8

Florence v. Bd. of Chosen Freeholders of Cnty. of Burlington,
566 U.S. ___, 132 S. Ct. 1510 (2012) 11, 12

Gracie v. State,
92 So.3d 806 (Ala. Crim. App. 2011) 8

Gustafson v. Florida,
414 U.S. 260 (1973) 4

Hill v. California,
401 U.S. 797 (1971) 11

Illinois v. Lafayette,
462 U S. 640 (1983) 2, 11

Knowles v. Iowa,
525 U.S. 113 (1998) 5

Maryland v. King,
___ U.S. ___, 133 S. Ct. 1958 (2013) . 3, 10, 11, 12

People v. Diaz,
244 P.3d 501 (Cal. 2011) 6

Sinclair v. State,
76 A.3d 442, (Md. App. 2013) 8

State v. Sizemore,
129 So.3d 860 (La. App. 2013) 9

United States v. Brown,
726 F.3d 993 (7th Cir. 2013) 7

United States v. Curtis,
635 F.3d 704 (5th Cir. 2011) 8

United States v. Edwards,
415 U.S. 800 (1974) 5

United States v. Flores-Lopez,
670 F.3d 803 (7th Cir. 2012) . . . . . *passim*

United States v. Gomez,
807 F. Supp. 2d 1134 (S.D. Fla. 2011) . . 6, 14, 15

United States v. Ham,
628 F.3d 801 (6th Cir. 2011) 7

United States v. Lustig,
___ F. Supp. 2d ___, 2014 WL 940502 (S.D. Cal. 2014) 9

United States v. McFarland,
633 F.2d 427 (5th Cir. 1980) 6

United States v. Murphy,
552 F.3d 405 (4th Cir. 2009) 9, 14, 15

United States v. Perez,
280 F.3d 318 (3d Cir. 2002) 7

United States v. Robinson,
414 U.S. 218 (1973) . . . . . *passim*

United States v. Santillan,
571 F. Supp. 2d 1093 (D. Ariz. 2008) 11

United States v. Shibin,
722 F.3d 233 (4th Cir. 2013) 8

United States v. Watson,
669 F.2d 1374 (11th Cir. 1982) 5

United States v. Willoughby,
742 F.3d 229 (6th Cir. 2014) 7

United States v. Wilson,
565 F.3d 1059 (8th Cir. 2009) 8

United States. v. Wurie,
728 F.3d 1 (1st Cir. 2013) 9, 10

Virginia v. Moore,
553 U.S. 164 (2008) 4

Washington v. Chrisman,
455 U.S. 1 (1982) 10

Weeks v. United States,
232 U.S. 383 (1914) 1

OTHER AUTHORITIES

3 W. LAFAVE, SEARCH AND SEIZURE § 5.2(c) (4th ed. 2004) 13

U.S. Dep't of Justice, Federal Bureau of Investigation, Uniform Crime Reports: Law Enforcement Officers Killed and Assaulted (2012) 10

INTEREST OF AMICI CURIAE

The amici States have a vital interest in ensuring their law enforcement officers are able to employ predictable, workable rules in the field. Searching an arrestee incident to an arrest is one such bright-line rule. Searches incident to arrest help preserve valuable evidence, which in turn enables the States to protect their citizens from dangerous offenders and punish those who disregard the law. Arrest-based searches also help ensure the safety of those tasked with enforcing the law, and may assist in correctly identifying arrestees who provide false identities to authorities. Thus, the amici States have a strong interest in ensuring their law enforcement officers are able to continue to conduct searches incident to arrest, regardless of the nature of the item searched. *See United States v. Robinson*, 414 U.S. 218, 224–37 (1973).

SUMMARY OF THE ARGUMENT

This Court has embraced the search-incident-to-arrest exception to the warrant requirement for over a century. *See Weeks v. United States*, 232 U.S. 383, 392 (1914) (stating that the right to search incident to an arrest has "always [been] recognized under English and American law"). The search of a person lawfully arrested is intended, in part, to "vindicate society's interest in having its laws obeyed" by preserving evidence. *Robinson*, 414 U.S. at 228 (quoting *Terry v. Ohio*, 392 U.S. 1, 26 (1968)). And, of course, a search incident to arrest—regardless of the nature of the offense—helps to ensure the safety of law enforcement officers. *Robinson*, 414 U.S. at 234–35 & n.5 (discussing the dangers police officers face during an arrest). The Court has also recognized that evidence

adduced from a search incident to an arrest may provide a "means of identifying the criminal." *Id.* at 232 (quoting *Holker v. Hennessey*, 42 S.W. 1090, 1093 (1897)). Given these weighty interests, the search-incident-to-arrest exception has long been recognized as providing a broad, "unqualified authority . . . to search the person of the arrestee." *Robinson*, 414 U.S. at 225; *Illinois v. Lafayette*, 462 U.S. 640, 644 (1983) (recognizing the search-incident-to-arrest exception extends to areas "within the arrestee's immediate control").

The importance of the search-incident-to-arrest exception is amplified, not diminished, by its application to new technology, including cell phones. Cell phones are not only capable of providing valuable evidence of a criminal offense, but are also often an instrumentality of a crime. Moreover, evidence on a cell phone is ephemeral and may be lost if officers are required to obtain a warrant before a search. Because the danger to police officers is at its pinnacle at the time of arrest, they should be able to take all reasonable measures to protect themselves, including searching a cell phone to help identify the arrestee and determine whether an arrestee's associates are in the area and pose a risk to them. These many justifications support this Court's continuing adherence to the "broadly stated" rule that a search incident to an arrest includes all items within an arrestee's immediate control. *Robinson*, 414 U.S. at 226.

Further, law enforcement officers need clear, workable rules in order to ensure their own safety, as well as to preserve evidence. Retreating from the broad rule recognized in *Robinson* because of the

capabilities of cell phones would require officers to make impromptu decisions regarding the appropriateness of a particular search based upon a myriad of factors associated with each particular arrest. The scope of the rule should not depend on the technological capability of a particular phone. Regardless of whether a phone is basic or "smart," the information on the phone is subject to loss unless officers can conduct an immediate search. It would also be unrealistic to require law enforcement officers to make on-the-spot determinations regarding the technological capability of a particular phone in order to later defend a search incident to arrest. Consequently, this Court should recognize that the contents of an arrestee's cell phone—like the contents of a notebook, ledger, wallet, diary, or other item under an arrestee's immediate control at the time of arrest—is subject to being searched as an incident of arrest.

ARGUMENT

THE SEARCH OF A CELL PHONE IS REASONABLE UNDER THE SEARCH-INCIDENT-TO-ARREST EXCEPTION TO THE WARRANT REQUIREMENT.

A. The Policies Furthered by the Broad Search-Incident-to-Arrest Exception Apply to the Contents of a Cell Phone.

In *Robinson*, this Court discussed the extended history of the search-incident-to-arrest exception, noting that its validity "has been regarded as settled from its first enunciation . . . ." 414 U.S. at 224–26; *see also Maryland v. King*, — U.S. —, 133 S. Ct. 1958, 1971

(2013) (stating that "[t]he validity of the search of a person incident to a lawful arrest . . . has remained virtually unchallenged") (quoting *Robinson*, 414 U.S. at 224); *Gustafson v. Florida*, 414 U.S. 260, 264–65 (1973) (noting the search-incident-to-arrest exception existed "both at common law and in the early development of American law"). The two principal justifications for the exception are the need to preserve evidence and the need to ensure the safety of the arresting officer. *Robinson*, 414 U.S. at 224–36; *see also Chimel v. California*, 395 U.S. 752, 763 (1969) (stating that the need to preserve evidence and the need for officer safety also allows for a search incident to arrest of items within an arrestee's "immediate control"). A third basis for the exception is to provide a "means of identifying the criminal." *Robinson*, 414 U.S. at 232 (quoting *Holker*, 42 S.W. at 1093).

The search-incident-to-arrest exception is expansive, and does not depend "on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect." *Robinson*, 414 U.S. at 235; *see also Arizona v. Gant*, 556 U.S. 332, 338–39 (2009) (noting that the search-incident-to-arrest exception "derives from interests in officer safety and evidence preservation that are *typically* implicated in arrest situations") (emphasis added); *Virginia v. Moore*, 553 U.S. 164, 177 (2008) ("The interests justifying [a] search [incident to an arrest] are present *whenever* an officer makes an arrest.") (emphasis added); *Robinson*, 414 U.S. at 237 (stating that if an "arrest is lawful, the privacy interest guarded by the Fourth Amendment is subordinated to a legitimate and overriding governmental concern . . . even if that

search is not narrowly limited by the twin rationales of seizing evidence and disarming the arrestee") (Powell, J., concurring).

Ultimately, *Robinson* recognized a police officer's "unqualified authority" to search upon a lawful custodial arrest. 414 U.S. at 229–30. Because this authority stems from the validity of the underlying arrest, the scope of the exception is necessarily broad and includes *any* item where evidence may be concealed. *See Knowles v. Iowa*, 525 U.S. 113, 118 (1998) ("In *Robinson*, we held that the authority to conduct a full field search as incident to an arrest was a 'bright-line rule,' which was based on the concern for officer safety and destruction or loss of evidence, but which did not depend in every case upon the existence of either concern."); *see also United States v. Edwards*, 415 U.S. 800, 803 (1974) ("It is also plain that searches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention.").

And, because there is broad authority to search for evidence of the crime, a search incident to an arrest necessarily entails an officer's ability to search documents and similar items that may provide evidence of a crime, even if personal information is revealed. *See, e.g., United States v. Flores-Lopez*, 670 F.3d 803, 807 (7th Cir. 2012) (stating that "opening the diary found on the suspect whom the police have arrested, to verify his name and address and discover whether the diary contains information relevant to the crime for which he has been arrested, clearly is permissible"); *United States v. Watson*, 669 F.2d 1374, 1384 (11th Cir. 1982) (stating that since a wallet "was

taken from [the defendant's] person during a search incident to arrest, [t]he seizure of documents found within the wallet was within the proper scope of the search") (internal citations omitted); *United States v. McFarland*, 633 F.2d 427, 429 (5th Cir. 1980) (rejecting as frivolous defendant's contention that the seizure of a piece of paper "was the product of an impermissibly broad search incident," noting that the very "purpose of the doctrine permitting searches incident to arrest is to allow discovery and preservation of destructible evidence"); *United States v. Gomez*, 807 F. Supp. 2d 1134, 1144 (S.D. Fla. 2011) ("Historically, . . . the broad grant of authority to search [incident to an arrest] includes highly private articles on a person like a wallet or purse, a briefcase, a backpack or personal bag, an address book or organizer, highly private places like a person's home closet . . . .") (collecting cases, footnotes omitted).

The data in a cell phone is not inherently more private than information on paper or in other documentary forms. A text or email message is essentially an electronic form of a letter or similar form of communication. *See Flores-Lopez*, 670 F.3d at 805 ("A modern cell phone is in one aspect a diary writ large."). Consequently, because there is no principled basis to distinguish a cell phone from any other item containing personal information, "the unqualified authority of the arresting authority to search the person of the arrestee," *Robinson*, 414 U.S. at 225, necessarily allows law enforcement officers to search the data in a cell phone. *See id.* (discussing "the *categorical* recognition of the validity of a search incident to lawful arrest") (emphasis added); *see also People v. Diaz*, 244 P.3d 501, 507 (Cal. 2011) ("Nothing

in [the Supreme Court's decisions on arrest-based searches] even hints that whether a warrant is necessary for a search of an item properly seized from an arrestee's person incident to a lawful custodial arrest depends in any way on the character of the seized item.").

B. No Principled Basis Exists to Exclude the Search of a Cell Phone from the Search-Incident-to-Arrest Exception.

There is no reason to find the search-incident-to-arrest exception inapplicable to cell phones placing them beyond the reach of this well-established law-enforcement tool. *See Robinson*, 414 U.S. at 225–26 (noting a police officer's "affirmative authority" "to find and seize things connected with the crime as its fruits or as the means by which it was committed") (quoting *Agnello v. United States*, 269 U.S. 20, 30 (1925)). Cell phones—including "throwaway phones"—are often used to facilitate criminal offenses, most typically drug offenses. *See, e.g.*, *United States v. Brown*, 726 F.3d 993, 996 (7th Cir. 2013) (noting that drug traffickers "frequently had couriers provide prepaid cell phones to their business associates to facilitate communication with [them]"); *United States v. Ham*, 628 F.3d 801, 805 (6th Cir. 2011) (citing testimony of DEA agent that "drug traffickers often use throw-away phones because they can be set up with a fictitious name, making them untraceable"); *United States v. Perez*, 280 F.3d 318, 342 (3d Cir. 2002) (reciting expert testimony presented to explain how drug traffickers use cell phones to frustrate police investigators).

Moreover, cell phones can provide critical evidence relating to a variety of crimes. *See, e.g.*, *United States*

v. Willoughby, 742 F.3d 229, 233–41 (6th Cir. 2014) (discussing how defendant used cell phone in furtherance of sex-trafficking of a minor); *United States v. Shibin*, 722 F.3d 233, 236–37 (4th Cir. 2013) (detailing how evidence relating to the defendant's cell phone tied him to a Somalian pirate attack of an American sailing ship); *United States v. Curtis*, 635 F.3d 704, 711 (5th Cir. 2011) (noting that the text messages of a defendant arrested on state-law charges led to evidence that the defendant was also involved in a federal fraud scheme); *United States v. Wilson*, 565 F.3d 1059, 1065 (8th Cir. 2009) (stating that a child sex abuse victim informed officers that the defendant "had used his cellular phone . . . to record her engaging in underage sexual activity"); *Gracie v. State*, 92 So.3d 806, 808 (Ala. Crim. App. 2011) (upholding cell phone search that showed bank robber texted an acquaintance immediately after the robbery and admitted his involvement); *Fawdry v. State*, 70 So.3d 626, 627 (Fla. App. 2011) (indicating that search of arrestee's phone "revealed images of child pornography"); *Sinclair v. State*, 76 A.3d 442, 447–54 (Md. App. 2013) (upholding search of defendant's cell phone, which provided evidence tying him to carjacking).

Valuable, and even crucial, evidence on a cell phone may be destroyed merely "by touching a button." *Flores-Lopez*, 670 F.3d at 807–08 (discussing "local wiping," where pressing a single button deletes a cell phone's contents). Also, a cell phone may "lock" after a certain period of time, rendering it impenetrable in the time it may take to obtain a search warrant. *Id.* at 807 (noting a phone may be "password-protected"). And more sophisticated means of destroying cell phone

evidence also exists, including "remote wiping," *i.e.*, deleting information on a phone from a remote location. *Id.* at 807–08 (stating that "remote-wiping capability is available on all major cell-phone platforms [and that] if the phone's manufacturer doesn't offer it, it can be bought from a mobile-security company");[1] *see also United States v. Lustig*, ___ F. Supp. 2d ____, 2014 WL 940502, at 4, & nn. 3–4 (S.D. Cal. 2014) (noting new technologies designed to prevent law enforcement officers from trying to preserve data on a cell phone).

Denying a law enforcement officer the ability to search a cell phone incident to arrest not only risks the destruction of the ephemeral information on the arrestee's phone, it may also result in the loss of other incriminating evidence. For instance, in the companion case to the instant case, the cell phone of an arrested drug dealer kept ringing after the defendant was arrested, indicating the phone was receiving calls from "[his] house." *United States. v. Wurie*, 728 F.3d 1, 2 (1st Cir. 2013). Using information they found on the phone, police officers responded to the arrestee's residence and secured it while they obtained a search warrant. *Id.* After the search warrant was obtained, the officers found, among other things, 215 grams of crack cocaine, a firearm, and ammunition. *Id.* If the

---

[1] For some cell phones, even this is unnecessary; instead, information may be deleted automatically when the phone receives new information. *See United States v. Murphy*, 552 F.3d 405, 411–12 (4th Cir. 2009) (discussing the potentially "volatile nature" of a cell phone, *i.e.*, the possibility that "information stored on a cell phone will be automatically deleted"); *see also State v. Sizemore*, 129 So.3d 860, 868 (La. App. 2013) (noting that text messages were lost due to an "auto-delete" setting on arrestee's phone).

officers had not searched the phone, the arrestee's failure to answer the phone could very well "have alerted [his] confederates to his arrest, prompting them to destroy further evidence of his crimes." *Id.* at 17 (Howard, J., dissenting).

Concerns for officer safety also support the reasonableness of searching cell phones incident to arrest. Law enforcement officers have inherently dangerous jobs. In 2012 alone "48 law enforcement officers died as a result of felonious acts," and more than 52,000 others were the "victims of line-of-duty assaults." U.S. Dep't of Justice, Federal Bureau of Investigation, Uniform Crime Reports: Law Enforcement Officers Killed and Assaulted (2012). This is stark evidence that "[e]very arrest must be presumed to present a risk of danger to the arresting officer." *Washington v. Chrisman*, 455 U.S. 1, 7 (1982). This danger "flows from the fact of the arrest, and its attendant proximity, stress, and uncertainty," not the particular underlying grounds for the arrest. *Robinson*, 414 U.S. at 234, n.5; *see also King*, 133 S. Ct. at 1971 ("It is a common occurrence that people detained for minor offenses can turn out to be the most devious and dangerous criminals.") (internal quotation marks omitted). Searching a cell phone incident to an arrest promotes officer safety by allowing officers to determine whether there is a possibility that an arrestee's cohorts may pose a danger.[2] *See, e.g.*, *United*

---

[2] The cell phone itself can even be used as a weapon. *See Farrington v. Smith*, 707 F.3d 963, 965-66 (8th Cir. 2013) (discussing the possibility that a cell phone may have been "weaponized" and turned into a handgun or that it may contain

States v. Santillan, 571 F. Supp. 2d 1093, 1102–04 (D. Ariz. 2008) (stating that search of arrestee's cell phone helped "to preserve safety" where the arrestee's armed cohorts remained at large).

Furthermore, this Court has noted that evidence adduced from such a search incident to arrest may provide a "means of identifying the criminal." *Robinson*, 414 U.S. at 232 (quoting *Holker*, 42 S.W. at 1093); *Lafayette*, 462 U.S. at 647 (noting that "inspection of an arrestee's personal property may assist the police in ascertaining or verifying his identity"); *Hill v. California*, 401 U.S. 797, 804 (1971) (stating that "aliases and false identifications are not uncommon" when a suspect is arrested). Searching a cell phone incident to arrest may, in some instances, further the important interest of identifying arrestees and ensuring they are processed in the criminal justice system under their correct name. *See King*, 133 S. Ct. at 1970 (noting the well-established need for law enforcement officers to accurately "process and identify the persons" they take into custody).

Finally, law enforcement officers have a responsibility to ensure that arrestees do not pose unwarranted "risks for facility staff" or "the existing detainee population." *Florence v. Bd. of Chosen Freeholders of Cnty. of Burlington*, 566 U.S. ___, 132 S. Ct. 1510, 1518 (2012). When an arrestee is correctly identified, his criminal history can be ascertained, which in turn allows a detention facility to make a more informed housing determination for the newly-

---

razor blades); *Flores-Lopez*, 670 F.3d at 806-07 (noting "[o]ne can buy a stun gun that looks like a cell phone").

arrived detainee. *See King*, 133 S. Ct. at 1971–72 ("A suspect's criminal history is a critical part of his identity that officers should know when processing him for detention."). Information discovered on a cell phone may also apprise authorities of an arrestee's gang affiliation and help ensure that rival gang members are not housed together. *See Florence*, 132 S. Ct. at 1518–19 (stating that "[j]ails and prisons also face grave threats posed by the increasing number of gang members who go through the intake process" and that "[t]he identification and isolation of gang members before they are admitted protects everyone in the facility"). In fact, the record in this case demonstrates that the officers were able to confirm Petitioner's gang affiliation upon a quick inspection of the phone at the scene of his arrest. Joint Appendix, at 8.

In sum, all of the considerations supporting the breadth of the search-incident-to-arrest exception apply with equal, if not greater, force to cell phones. A search of a cell phone incident to arrest is reasonable and not prohibited by the Fourth Amendment. *See Robinson*, 414 U.S. at 236 (holding that "in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment").

C. Law Enforcement Officers Need Clear Workable Rules, Like the One Articulated in *Robinson*.

Law enforcement officers have inherently dangerous jobs and routinely react to rapidly developing situations. This Court has recognized that the danger to a police officer is perhaps at its greatest during an

arrest. *Robinson*, 414 U.S. at 234 & n.5. To provide a straightforward and predictable rule in this context, law enforcement officers must be allowed to search all items under an arrestee's immediate control—including cell phones—as part of a search incident to arrest. *See Dunaway v. New York*, 442 U.S. 200, 213–14 (1979) ("A single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront."); *see also* 3 W. LAFAVE, SEARCH AND SEIZURE § 5.2(c), at 106–07 (4th ed. 2004) ("A highly sophisticated set of rules [for police officers], qualified by all sorts of ifs, ands and buts and requiring the drawing of subtle nuances and hairline distinctions, may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be literally impossible of application by the officer in the field.").

Robinson itself recognizes the need for a bright-line rule for arrest-based searches: "A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search." 414 U.S. at 235; *see also id.* at 225 (discussing "the categorical recognition of the validity of a search incident to lawful arrest"). Retreating from the broad rule stated in *Robinson* based on the capabilities of new technology would expose the decisions of police officers to second-guessing, and subject their on-the-spot judgment to post hoc judicial weight of such factors as the possibility that invaluable evidence will be destroyed,

officer safety issues, and concerns about an arrestee's true identity. A fact-based approach to determine the validity of a search incident to arrest would only add uncertainly to the already unpredictable nature of an arrest.

The reasonableness of the warrantless search of a cell phone does not depend on the technological capabilities of a particular phone. In one case, the defendant argued "that whether a cell phone may be searched without a warrant can be determined only upon the officers ascertaining the cell phone's storage capacity." *Murphy*, 552 F.3d at 411. Under that defendant's theory, a phone with "a small storage capacity may be searched without a warrant due to the volatile nature of the information stored,[3] but a search of a cell phone with a larger storage capacity would implicate a heightened expectation of privacy and thus would require a warrant to be issued before a search could be conducted." *Id.* Courts cannot reasonably expect law enforcement officers to make accurate on-the-spot determinations concerning a cell phone's capabilities in order to assess the risk that electronic evidence may be lost in the time it takes to obtain a

---

[3] This apparently refers to phones with limited capacity where the receipt of new information deletes existing information. This particular concern appears to be waning. *See Gomez*, 807 F. Supp. 2d at 1150 n. 17 (stating that it is unlikely that "a modern cell phone, with its continually advancing technology, is at any risk of deleting its call history or text messages folder to make space for incoming calls or text messages"). Nonetheless, information on a cell phone is still volatile given the very real possibility of local or remote "wiping." While the degree of volatility depends on the capabilities of a particular phone, those capabilities are not readily or necessarily apparent to arresting officers.

search warrant. A rule requiring an officer to determine the capability of a particular cell phone before a search is simply unworkable and unreasonable. *See Murphy*, 552 U.S. at 411 (stating that "to require police officers to ascertain the storage capacity of a cell phone before conducting a search would simply be an unworkable and unreasonable rule," that could result in the permanent loss of evidence); *see also Gomez*, 807 F. Supp. 2d at 1150 & n.16 (stating that crafting a specific rule for the search of a cell phone "is very difficult," and the problem "is exacerbated by the continually advancing technology and computing capabilities of hardware, such as 'smart' phones").

Consequently, for all the above reasons, this Court should not retreat from *Robinson's* bright-line rule that all items within an arrestee's immediate control—including a cell phone—may be searched incident to a lawful arrest.

CONCLUSION

This Court should affirm the state court's decision and hold that the search of a cell phone's contents falls within the search-incident-to-arrest exception to the Fourth Amendment.

Respectfully submitted this 9th day of April, 2014.

THOMAS C. HORNE
Arizona Attorney General
ROBERT L. ELLMAN
Solicitor General
JOSEPH T. MAZIARZ
Chief Counsel, Criminal Appeals Section
MICHAEL T. O'TOOLE
Assistant Attorney General
Counsel of Record
1275 West Washington Street
Phoenix, AZ 85007
Phone (602) 542-8551
Fax (602) 542-4849
michael.otoole@azag.gov
Counsel for Amici Curiae

AMICUS CURIAE BRIEF

Supreme Court, U.S.
FILED
APR 9 - 2014
OFFICE OF THE CLERK

No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari To The California Court of Appeal, Fourth Appellate District

BRIEF OF *AMICI CURIAE* ASSOCIATION OF STATE CRIMINAL INVESTIGATIVE AGENCIES, INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, NATIONAL SHERIFFS' ASSOCIATION, MAJOR CITY CHIEFS ASSOCIATION, MAJOR COUNTY SHERIFFS' ASSOCIATION, ASSOCIATION OF PROSECUTING ATTORNEYS, AND ROCKLAND COUNTY DISTRICT ATTORNEY, IN SUPPORT OF RESPONDENT

GAËTAN GERVILLE-RÉACHE
COUNSEL OF RECORD
JOHN J. BURSCH
MATTHEW T. NELSON
WARNER NORCROSS & JUDD LLP
900 Fifth Third Center
111 Lyon Street N.W.
Grand Rapids, MI 49503
(616) 752-2000
greache@wnj.com

QUESTION PRESENTED

Whether the officers' searches of the cell phone seized incident to petitioner's arrest were lawful under the Fourth Amendment.

TABLE OF CONTENTS

INTEREST OF THE *AMICI CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 4

STATEMENT 5

ARGUMENT 7

I. This Court's precedent and sound policy support the warrantless search of a cell phone incident to arrest 7

A. Smartphone data is highly susceptible to destruction 8

B. Smartphones pose time-sensitive accessibility problems that justify an immediate search 10

C. Tracking features activated by later searches can compromise investigations and officer safety 11

D. Smartphones pose unique evidence-preservation and officer-safety challenges that make a case-by-case assessment unrealistic 12

II. At a minimum, the Court should reject Petitioner's request for a blanket prohibition on cell phone searches incident to arrest 14

CONCLUSION 17

TABLE OF AUTHORITIES

Page(s)

Cases

Arizona v. *Gant*,
556 U.S. 332 (2009) 14, 15

Graham v. *Connor*,
490 U.S. 386 (1989) 12

Harris v. *United States*,
331 U.S. 145 (1947) 8

People v. *Diaz*,
51 Cal. 4th 84, 244 P.3d 501 (2011) 6

People v. *Riley*,
2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013) 7

Thornton v. *United States*,
541 U.S. 615 (2004) 7

United States v. *Carrion*,
809 F.2d 1120 (5th Cir. 1987) 16

United States v. *Chadwick*,
433 U.S. 1 (1977) 6

United States v. *Diaz-Lizaraza*,
981 F.2d 1216 (11th Cir. 1993) 16

United States v. *Edwards*,
415 U.S. 800 (1974) 6, 8

United States v. *Frankenberry*,
387 F.2d 337 (2d Cir. 1967) 16

United States v. *Ortiz*,
84 F.3d 977 (7th Cir. 1996) 16

TABLE OF AUTHORITIES—Continued

Page(s)

United States v. *Robinson*,
414 U.S. 218 (1973) 6, 7

United States v. *Smith*,
565 F.2d 292 (4th Cir. 1977) 16

United States v. *Uricoechea-Casallas*,
946 F.2d 162 (1st Cir. 1991) 16

United States v. *Watson*,
669 F.2d 1374 (11th Cir. 1982) 16

Weeks v. *United States*,
232 U.S. 383 (1914) 7, 15

Other Authorities

Sean Morrissey, *iOS Forensic Analysis for iPhone, iPad and iPod touch* (2010) 10, 15

INTEREST OF THE *AMICI CURIAE*[1]

The Association of State Criminal Investigative Agencies is composed of 39 state criminal investigative agencies, including state divisions/bureaus of criminal investigation and state police agencies. As the representative of the law enforcement officials who daily put their lives on the line to protect the public and solve crimes, the Association has an intense interest in law enforcement's ability to quickly and accurately collect information that will protect the public, ensure officer safety, and enable the successful prosecution of criminals.

Founded in 1893, the International Association of Chiefs of Police (IACP), with more than 22,000 members in 101 countries, is the world's oldest and largest association of police executives. IACP's mission, throughout the history of the association, has been to identify, address, and provide solutions to urgent law-enforcement issues. IACP represents the interests of law-enforcement agencies at the federal, state, and local levels. Association members include law-enforcement officers and law-enforcement administrators who are charged with the responsibility of protecting citizens from criminals, both nationally and internationally.

The National Sheriffs' Association, a 26 U.S.C. § 501(c)(4) non-profit, was formed in 1940 to promote

---

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief.

the fair and efficient administration of criminal justice and protect the Office of Sheriffs. The Association has over 21,000 members and is the advocate for over 3,000 sheriffs located throughout the United States. The National Sheriffs' Association promotes the public-interest goals and policies of law enforcement in the nation, and it participates in judicial processes where the vital interests of law enforcement and its members are being affected.

The Major City Chiefs Association is a professional association of Chief police executives representing the largest cities in the United States, Canada, and the United Kingdom. MCCA membership comprises Chiefs and Sheriffs of the 66 largest law-enforcement agencies in the United States, nine largest in Canada and two in the United Kingdom. They serve 89.9 million people (69.5 US; 10.5 Canada; 9.9 UK) with a sworn workforce of 239,063 (161,664 US; 20,506 Canada; 56,893 UK) officers and non-sworn personnel.

The Major County Sheriffs' Association, a 26 U.S.C. § 501(c)(4) non-profit, is an association of elected sheriffs representing the nation's largest counties with populations of 500,000 people or more, serving over 100 million Americans. The Major County Sheriffs' Association works to promote a greater understanding of law-enforcement strategies to address future problems and identify law-enforcement challenges facing the members of its organization.

The Association of Prosecuting Attorneys (APA) was founded as a national organization to represent all prosecutors and provide additional resources such as training and technical assistance in an effort to develop proactive and innovative prosecutorial practices that prevent crime, ensure equal justice, and

make our communities safer. The APA acts as a global forum for the exchange of ideas, allowing prosecutors to collaborate with each other and other criminal-justice partners. The APA also serves as an advocate for prosecutors on emerging issues related to the administration of justice, among other ways by submitting briefs as *amicus curiae* in appropriate cases. The APA's board of directors includes current elected prosecutors from different states throughout the nation.

The Rockland County District Attorney's Office has the responsibility and authority to both investigate and prosecute crimes and offenses in Rockland County and undertake all efforts necessary to proactively prevent the commission of crimes. Rockland County is a suburb located about 25 miles from New York City. Rockland's law-enforcement community is typical of smaller jurisdictions that lack the manpower and fiscal resources that many larger jurisdictions possess. Thus, rules that further local law enforcement's ability to quickly gather information as incidents occur are paramount to both protecting local residents and prosecuting offenders. Limitations of the kind contemplated in this case often have an outsized effect on smaller jurisdictions.

INTRODUCTION AND SUMMARY OF ARGUMENT

Petitioner Riley asks this Court for a blanket rule that "when officers seize smart phones incident to lawful arrests, they may not search the phones' digital contents without first obtaining a warrant." Pet. 3. Such a rule is inconsistent with this Court's precedents and is bad public policy.

Consider police officers who pull alongside a sedan parked near a local courthouse. The officers observe bomb-making materials in the front seat, two steaming cups of coffee, and a single passenger—the driver—who is frantically sending a text message on his smartphone. The officers have probable cause to arrest. But if they are barred from examining the phone without first obtaining a warrant, they will be unable to locate and stop the driver's accomplice—the bomber—who is preparing to detonate a bomb inside the courthouse.

Or imagine officers responding to an APB who arrest a man matching the description of a known child predator. The arrestee's smartphone holds an email that contains the address of a young child who has been kidnapped and is being abused by the arrestee's accomplice. But by the time the officers obtain a warrant and arrive on the scene, the child has been removed to another location or murdered.

Such exigencies go far beyond the immediate safety of officers and members of the public. If officers arrest a man as part of a routine traffic stop, he may call an accomplice with his "one phone call" to remotely erase all the contents of his smartphone before the police can obtain a warrant to search it, that would have revealed thousands of pictures and videos containing child pornography.

The above scenarios are all hypothetical. But the anecdotes set forth below are not; they arise from real cases involving real criminal acts and evidence. The anecdotes demonstrate that there is a compelling governmental interest in searching cell phones incident to arrest in all cases, an interest that, as with any search incident to arrest, overcomes any expectation of privacy in personal effects. Accordingly, the Court should affirm the California Supreme Court and hold that officers may search smartphones incident to arrest without first obtaining a warrant. Alternatively, and at a bare minimum, the Court should grant law enforcement officials the leeway to search cell phones incident to arrest when they have reason to believe the phones contain evidence of past, present, or future crime.

STATEMENT

San Diego police officers stopped petitioner Riley due to expired registration tags on the car he was driving. During the stop, the officers discovered Riley was driving with a suspended license and impounded the car. A standard inventory search revealed two loaded firearms, hidden in the engine compartment. The police arrested Riley.

In the officers' search incident to their arrest of Riley, an officer cursorily examined the address book in Riley's cell phone and saw that a number of entries started with "ck," a well-known mark that Blood gang members use to signify "Crip Killer."

At the police station, a supplemental review of Riley's cell phone revealed videos and pictures of gang activity. And the police later learned—through means not at issue here—that Riley's cell phone had been used near the location of a shooting that caused a Crip gang member to drive off the road and crash his car.

Additional evidence at trial established that Riley and fellow Lincoln Park gang members were in fact involved in that shooting. A jury convicted Riley of shooting at an occupied vehicle, attempted murder, and assault with a semiautomatic firearm.

The trial court denied Riley's motion to suppress the cell phone evidence based on *People* v. *Diaz*, 51 Cal. 4th 84, 93, 244 P.3d 501 (2011). The California Supreme Court in *Diaz*, relying on this Court's decisions in *United States* v. *Robinson*, 414 U.S. 218 (1973), *United States* v. *Edwards*, 415 U.S. 800 (1974), and *United States* v. *Chadwick*, 433 U.S. 1 (1977), determined that the cell phone was appropriately searched:

> [T]he key question in this case is whether defendant's cell phone was "personal property . . . immediately associated with [his] person" (*Chadwick*, *supra*, 433 U.S. at p. 15) like the cigarette package in *Robinson* and the clothes in *Edwards*. If it was, then the delayed warrantless search was a valid search incident to arrest. [*Diaz*, 244 P.3d at 505.]

The *Diaz* court concluded that the phone was personal property on the defendant's person at the time of his lawful arrest and was therefore subject to search under this Court's precedents.

Riley appealed his conviction, and the California Court of Appeals affirmed. That court held that *Diaz* controlled, and that the search of Riley's phone was a valid search incident to arrest because the phone "was 'immediately associated' with [Riley's] 'person' when he was stopped." *People* v. *Riley*, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013). The California Supreme Court denied Riley's petition for review without comment.

ARGUMENT

I. THIS COURT'S PRECEDENT AND SOUND POLICY SUPPORT THE WARRANTLESS SEARCH OF A CELL PHONE INCIDENT TO ARREST.

This Court in *United States* v. *Robinson*, 414 U.S. 218 (1973), recognized that a search incident to arrest includes police authority to search any items found on the arrestee, and a more limited authority to search the surrounding area. 414 U.S. at 224. The first authority flows from "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidence of crime." *Weeks* v. *United States*, 232 U.S. 383, 392 (1914). The law enforcement interest at stake is "gathering evidence relevant to the crime for which the suspect had been arrested." *Thornton* v. *United States*, 541 U.S. 615, 629 (2004) (Scalia, J., concurring in the judgment). And that interest is particularly compelling in the context of smartphones.

With respect to the authority to search the surrounding area, police conduct is more circumscribed. But the historical reason for such a search—"to find and seize things connected with the crime as its fruits or as the means by which it was committed," *Harris* v. *United States*, 331 U.S. 145, 152–53 (1947)—is again directly applicable to smartphones.

Cell phones are unique, however, in that their data can be erased remotely or become inaccessible due to encryption or a passcode in relatively short order. This presents challenges for law enforcement unparalleled in any other context this Court has dealt with previously. As explained below, this challenge can only be met by placing the search of a smartphone incident to arrest within the search-incident-to-arrest doctrine this Court articulated in *Robinson* and *United States* v. *Edwards*, 415 U.S. 800 (1974).

A. SMARTPHONE DATA IS HIGHLY SUSCEPTIBLE TO DESTRUCTION.

It is true that smartphones can contain a broad variety of personal information. It is equally true that smartphones can contain a broad variety of criminal evidence, from photos, to videos, to text messages. Critically—and very unlike traditional personal property—the memory on a cell phone can be erased (wiped) remotely with a simple command.[2]

---

[2] There is even a smartphone app being developed (Zones) that would wipe a phone's memory based on when the phone is carried into certain locations—such as a police station. Chirgwin, *WhisperSystems creates "suicide pill" for phones*, The Register (Jan. 28, 2014), www.theregister.co.uk/2014/01/28whisper systms_creates_suicide_pill_for_phones/.

A criminal caught with incriminating letters in his coat pocket can do nothing to destroy the letters once the police have taken possession of him. The same criminal with incriminating emails on his smartphone can place his one phone call at the police station to an accomplice who will remotely erase those emails with the swipe of a button. And such evidence destruction is hardly theoretical.

In Orange County, California, the Sheriff's Office was involved in an investigation of a county-wide criminal organization involving narcotic sales and money laundering, tied to storefront marijuana dispensaries. While the Sheriff's Office executed search warrants against the organization, its members were told to immediately destroy all digital documentation on their cell phones.

A later investigation revealed that the members' cell phones contained conversations and records that detailed the organization's criminal activity. Numerous defendants of the organization later admitted that they had a security procedure, complete with an IT department, to immediately and remotely wipe all digital information from their cell phones. All but one cell phone obtained during the Sheriff's Office raid had its contents wiped before search warrants were issued to recover the contents.

In Houston, Texas, while conducting a narcotics investigation, officers arrested Heather Garrett for evading arrest and for assaulting a public servant with her vehicle as she attempted to escape. Upon arrest, they learned that Garrett was a prostitute and worked for a "pimp" named Marcus Barnes. Officers found Garrett's "Backpage.com" listing, and learned that she used her phone to arrange sexual transactions and to communicate with Barnes. Police

seized Garrett's phone for possible follow-up investigation, and planned to request a warrant to search the phone to aid in a long-term investigation of multiple suspects. But after Garrett was booked, officers discovered that Garrett's phone had been erased remotely. There was no information on the phone; it had been restored to its factory settings.

Had law enforcement in the above examples searched the phones as an incident to arrest, they would have discovered critical information in furtherance of their investigations. Because they delayed to obtain a warrant, the criminals destroyed the evidence. Allowing an immediate search while the suspect is in custody, before the suspect receives his obligatory phone call, and before a cohort suspects his missing comrade has been arrested, ensures that electronic data is preserved.

B. SMARTPHONES POSE TIME-SENSITIVE ACCESSIBILITY PROBLEMS THAT JUSTIFY AN IMMEDIATE SEARCH.

Many cell phones have password locks that trigger automatically after several minutes of non-use. When the lock is triggered, all data on the device can become encrypted. A low battery can also lead to a cell phone losing power and becoming locked or encrypted during the time it would take to obtain a search warrant. Officers can bypass the password lock on some cell phone models using a device such as the Universal Forensic Extraction Device (UFED) for immediate acquisition. See generally www.cellebrite.com. On other cell phones (particularly iPhones), they cannot. Sean Morrissey, *iOS Forensic Analysis for iPhone, iPad and iPod touch* 87 (2010).

Given the speed with which cell phone technology advances, the constant revisions to smartphone software, the proliferation of various smartphone models, and the customization offered on the various models, it is unrealistic to expect officers spending long hours on their beat to also remain up to date on all of the latest technological developments, and anticipate in every given situation which phones can be accessed and wiped remotely, which can become password protected remotely, and how much time it takes for the password protection and encryption to take effect. This makes a case-by-case assessment of the exigency of each search highly impractical.

C. Tracking features activated by later searches can compromise investigations and officer safety.

Loss of access to crucial evidence on the phone is not the only reason for a blanket rule permitting a search incident to arrest. Delaying the search until after a warrant is obtained can tip off cohorts using the phone's GPS tracking, resulting in the organization's precautionary destruction of evidence elsewhere, or worse, creating a target for the organization's desperate and dangerous attempt to recover the phone and prevent the search.

Although law enforcement officers frequently attempt to keep seized cell phones from connecting to cellular or data networks, that is not always technically or operationally possible. Consider a situation where one member of a drug cartel is arrested and his phone confiscated. Officers immediately turn it off to prevent a cellular connection.

While back at the station, after a few hours, officers finally obtain a warrant to search the phone and turn it on to download the information that could lead to the location and arrest of other members. While it is on, and despite the officers' best efforts, the device connects to a cellular or data network. The suspect's superior, who is tracking the member's whereabouts using the Find iPhone app or similar app, discovers the phone is located at a police station, and executes their protocol for immediately removing the operation to a new, unknown location, thwarting the investigation and the opportunity for a major drug bust.

D. SMARTPHONES POSE UNIQUE EVIDENCE-PRESERVATION AND OFFICER-SAFETY CHALLENGES THAT MAKE A CASE-BY-CASE ASSESSMENT UNREALISTIC.

The ephemerality of cell phone data, accessibility problems, and special dangers inherent in searching cell phone data, make case-by-case search decisions impractical for officers in the field. Officers must often make "split-second judgments—in circumstances that are tense, uncertain, and rapidly evolving." *Graham* v. *Connor*, 490 U.S. 386, 396–97 (1989). It is not realistic to expect them to be able to make case-by-case search decisions given the prevalence of cell phones with encryption and password locks and remote wiping, when the window for decision may often be a matter of minutes or less.

In addition to racing against a potential password lock, arrests, and in particular traffic stops, are often conducted in public view, where an unknown accomplice or member of the arrestee's gang can see the arrest taking place and quickly destroy the evidence on the phone remotely without any cues from

the arrestee. This adds particular urgency that is difficult to calculate and assess as the scene develops and information becomes available during the stop or arrest. Failure to search the cell phone in time can mean the loss of access to time-sensitive evidence of a crime, which the officers would have cause to retrieve moments later when they discover there is more to the traffic stop than expired plates.

This particular case provides a keen example. It was not until officers conducted the inventory search that they discovered firearms hidden in a manner that gave them cause to believe Petitioner Riley was involved in gang activity and search the phone for those connections. Fortunately, the evidence of the criminal activity was not destroyed before officers discovered firearms in their routine inventory. But that was a distinct possibility. By searching the phone at the scene, officers minimized the risk that evidence of an attempted murder would be destroyed.

Contrary to what the Petitioner and *Amici* assert, an immediate search—rather than waiting the several hours it can take to obtain a warrant—is the only way to fully protect law enforcement's profound interest in preventing destruction of such evidence.

The Brief of *Amicus Curiae* Electronic Privacy Information Center discusses a number of low-cost techniques and tools for preventing a "wipe" signal from reaching the phone until a warrant can be obtained. But turning off the phone (which could encrypt and lock the data), removing the battery (which also could encrypt and lock the data), or enclosing it in a Faraday bag or something like it (which can occasionally leak a cellular signal), would

only work until the bag must be opened and the phone turned on to connect it to an extraction device.

At that point, and despite efforts to keep such devices from connecting to a network, the phone may become immediately vulnerable to a remote "kill pill" signal. Even if the connection lasts only a moment, that will instantly trigger destruction of all evidence on the phone or expose the cell phone's location.[3] Thus, any delay in searching the phone inevitably creates an opportunity for a cohort or the suspect (if, for example, bail is posted before a warrant issues) to destroy evidence or possibly endanger the safety of law-enforcement agents.

II. AT A MINIMUM, THE COURT SHOULD REJECT PETITIONER'S REQUEST FOR A BLANKET PROHIBITION ON CELL PHONE SEARCHES INCIDENT TO ARREST.

Even if the Court creates a special constitutional exception for smartphones, the Court should reject the categorical bar that Riley requests. When there are important law-enforcement justifications for such a search, officers should be able to conduct a search.

Consider this Court's decision in *Arizona* v. *Gant*, 556 U.S. 332 (2009). There, this Court held that a search incident to arrest does not categorically include a vehicle passenger compartment after the arrestee has already been placed in an officer squad car. But the Court still acknowledged that officers

---

[3] *Amici* also mention the option of using a Sensitive Compartmented Information Facility or SCIF. But this is anything but a low-cost option and is cost-prohibitive for most law-enforcement agencies. See www.adamoconstruction.com/what-is-scif.php.

could conduct a "search incident to arrest when it is reasonable to believe that evidence of the offense of arrest might be found in the vehicle." 556 U.S. at 335.

The circumstances here are far more compelling than in *Gant*, because, unlike the defendant in *Gant*, Petitioner Riley did not need to be near the evidence in his cell phone to destroy it. As explained above, he, or a passing friend, family member, or gang member could accomplish that task remotely. Thus, to actually "seize the fruits or evidence of crime," *Weeks*, 232 U.S. at 392—that is, wrest it from the arrestee's control to prevent its destruction—law enforcement must be allowed to immediately search the phone and, ideally, download the information to a secure location.

This can be accomplished almost immediately in the field, or in relatively short order at the station, with a Universal Forensic Extraction Device. With many (but not all) cell phone models, the UFED can bypass the access code and then download the data to a USB flash device or other electronic storage. See Sean Morrissey, *iOS Forensic Analysis for iPhone, iPad and iPod touch* 25 (2010). Critically, and contrary to what certain *Amici* suggest, this is *not* a search of private information on remote servers; it is only a transfer of data actually on the phone, which places the data in a secure location where it cannot be destroyed remotely.

The problem is particularly acute for those models whose password encryption cannot be bypassed. Accessing the phone immediately can be crucial to avoiding a password lock. With iPhones, for instance, the password lock can only be bypassed and the data accessed by Apple at its headquarters in Cupertino,

California. According to recent reports, Apple takes approximately two months simply to process the legal requests, and several additional months to actually access and acquire the data and submit the results to the requesting law enforcement agency.

If an iPhone is accessible due to recent use by the arrestee, there may be little time before the password lock takes effect. When officers have reason to believe the phone contains evidence of a crime, it makes no sense to require the officer to nevertheless obtain a search warrant, send the phone to Cupertino, California for evidence collection, and then wait months for results. This places an unreasonable burden on law enforcement's compelling interest in the rapid retrieval of evidence that could lead to the successful prosecution of criminals, prevent future crimes, and ensure public safety.

* * *

Under well-established circuit precedent, officers can already search a wide variety of personal items seized from a person at the time of his arrest. Such searches can and often will reveal embarrassing personal information about the arrestee. E.g., *United States* v. *Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996); *United States* v. *Diaz-Lizaraza*, 981 F.2d 1216, 1223 (11th Cir. 1993) (pager, address book, wallet); *United States* v. *Uricoechea-Casallas*, 946 F.2d 162, 166 (1st Cir. 1991) (wallet); *United States* v. *Carrion*, 809 F.2d 1120, 1123, 1128 (5th Cir. 1987) (address book); *United States* v. *Watson*, 669 F.2d 1374, 1383–84 (11th Cir. 1982) (address book, papers); *United States* v. *Smith*, 565 F.2d 292, 294 (4th Cir. 1977) (address book); *United States* v. *Frankenberry*, 387 F.2d 337, 339 (2d Cir. 1967) (diary).

Smartphones should be treated no differently. Accordingly, the Court should uphold the ability of law-enforcement officials to search cell phones incident to arrest, particularly when the information collected comes only from the cell phone and not remote servers.

If, however, the Court should find that cell phones are somehow different than traditional wallets, purses, diaries, papers, and address books, the Court should, at a bare minimum, recognize an officer's authority to search a smartphone without a search warrant when the officer has reason to believe the smartphone may contain evidence of a crime.

CONCLUSION

The judgment of the California Court of Appeals should be affirmed.

Respectfully submitted,

GAETAN GERVILLE-REACHE
COUNSEL OF RECORD
JOHN J. BURSCH
MATTHEW T. NELSON
WARNER NORCROSS & JUDD LLP
900 Fifth Third Center
111 Lyon Street N.W.
Grand Rapids, MI 49503
(616) 752-2000
greache@wnj.com

Counsel for Amici Curiae *ASCIA et al.*

April 2014

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
MAR 10 2014
OFFICE OF THE CLERK

No. 13-132

IN THE

SUPREME COURT OF THE UNITED STATES

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari to the California Court of Appeal, Fourth District

---

BRIEF FOR THE CATO INSTITUTE AS *AMICUS CURIAE* IN SUPPORT OF THE PETITIONER

JIM HARPER
Counsel of Record
ILYA SHAPIRO
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, D.C. 20001
(202) 842-0200
jharper@cato.org

Counsel for Amicus Curiae

Library of Congress
Law Library

QUESTION PRESENTED

Whether evidence admitted at petitioner's trial was obtained in a search of petitioner's cell phone that violated petitioner's Fourth Amendment rights.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

TABLE OF AUTHORITIES iv

INTEREST OF *AMICUS CURIAE* 1

SUMMARY OF THE ARGUMENT 1

ARGUMENT 2

I. THE COURT SHOULD ANALYZE DISTINCTLY EACH SEIZURE AND SEARCH THAT OCCURED IN THIS CASE 2

A. "Seizure" and "Search" Are Distinct Activities, Even if They Are Often Used Together to Investigate Suspects 3

B. The Investigation and Arrest of Riley Was a Series of Seizures and Searches 6

II. THIS COURT SHOULD RECOGNIZE THAT PHONES ARE THEMSELVES FOURTH AMENDMENT "EFFECTS," AND THAT PHONES CONTAIN FOURTH AMENDMENT PAPERS AND EFFECTS 10

A. A Cell Phone is an "Effect" Under the Fourth Amendment. 10

B. Among Other Content of the Cell Phone Were Constitutional "Papers and Effects" 11

III. NEITHER SEARCH OF RILEY'S CELL PHONE WAS JUSTIFIED BY THE *CHIMEL* FACTORS 15

A. The Exceptions to the Warrant Requirement for Searches Incident to Arrest Do Not Apply to Digital Searches 16

1. Digital Data is No Threat to Officers. 18

2. There was No Threat of Evidence-Destruction 20

CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

CASES

Arizona v. Gant,
556 U.S. 332 (2009) 15,17,19

Arizona v. Hicks,
480 U.S. 321 (1987) 3

Brendlin v. California,
551 U.S. 249 (2007) 6

Chimel v. California,
395 U.S. 752 (1969) .....*passim*

Closson v. Morrison,
47 N.H. 482 (NH 1867)..... 18

Ex Parte Jackson,
96 U.S. 727 (1877) 12

Hawkins v. Georgia,
290 Ga.. 785 (Georgia 2012)..... 17

Illinois v. Lafayette,
462 U.S. 640 (1983) 8

Illinois v. McArthur,
531 U.S. 326 (2001) 21

Kentucky v. King,
131 S.Ct. 1849 (2011) 23

Ker v. California,
374 U.S. 23 (1963) 23

Kyllo v. United States,
533 U.S. 27 (2001) 4,6,14

Massachusetts v. Phifer,
463 Mass. 790, (Mass. 2012) 17

New York v. Class,
475 U.S. 106 (1986) 3

Oliver v. United States,
466 U.S. 170 (1984) 5

Olmstead v. United States,
277 U.S. 438 (1928) 12

Ontario v. Quon,
560 U.S. 746 (2010) 25

People v. Chiagles,
237 N.Y. 193 (N.Y. 1923)..... 21

People v. Diaz,
244 P.3d 501 (Cal. 2011) 15,17

People v. Riley, 2013 Cal. App. Unpub.,
LEXIS 1033 (Cal. 2013).....7,8,15

Soldal v. Cook County,
506 U.S. 56 (1992) 4

South Dakota v. Opperman,
428 U.S. 364 (1976) 6,7

Terry v. Ohio,
392 U.S. 1 (1968) 6

Trupiano v. United States,
334 U.S. 699 (1948) 16

United States v. Chadwick,
433 U.S. 1 (1977) 10,17,21

United States v. Flores-Lopez,
670 F.3d 803 (7th Cir. 2012) 21

United States v. Jacobsen,
466 U.S. 109 (1984) 3,4

United States v. Jones,
132 S. Ct. 945 (2012) 3,6,10

United States v. Karo,
468 U.S. 705 (1984) 4

United States v. Place,
462 U.S. 696 (1983) 4

United States v. Quintana,
594 F. Supp. 2d 1291 (M.D. Fla. 2008) 23

United States v. Robinson,
414 U.S. 218 (1973) 16,17,20

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 14

Weeks v. United States,
232 U.S. 383 (1914) 20

Welsh v. Wisconsin,
466 U.S. 740 (1984) 23

Wong Sun v. United States,
371 U.S. 471 (1963) 23

STATUTES

Act of Feb. 20, 1792, § 16 11

OTHER AUTHORITIES

Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 Stan. L. Rev. 553 (2007) 11

BLACK'S LAW DICTIONARY (6th ed. 1990) 8,10

Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, *Report of the Civil Rules Advisory Committee 2*, May 27, 2005. *Available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV5-2005.pdf. 13

GERALD W. BROCK, *The Second Information Revolution* (Harvard University Press 2003) 12

JPEG Homepag , http://www.jpeg.org/jpeg/, (last visited March 9, 2014) 15

Lewis Coe, THE TELEGRAPH: A HISTORY OF MORSE'S INVENTION AND ITS PREDECESSORS IN THE UNITED STATES (McFarland and Co. 1993) 12

Mallory Simon, *Student 'Twitters' his way out of Egyptian Jail*, CNN.com (2008)

http://www.cnn.com/2008/TECH/04/25/twitter.buck/index.html 18

Mary Czerwinski et al., *Digital Memories in an Era of Ubiquitous Computing and Abundant Storage*, Communications of the ACM 45, Jan. 2006, *available at* http://research.microsoft.com/pubs/79673/CACMJan2006DigitalMemories.pdf 13

TONY HONORÉ, *Ownership*, in OXFORD ESSAYS ON JURISPRUDENCE (A.G. Guest ed., 1961) 5,9

INTEREST OF AMICUS CURIAE[1]

The Cato Institute was established in 1977 as a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Center for Constitutional Studies was established in 1989 to promote the principles of limited constitutional government that are the foundation of liberty. Toward those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs. The present case centrally concerns Cato because it represents an opportunity to improve Fourth Amendment doctrine and maintain that provision's protections in the modern era.

SUMMARY OF THE ARGUMENT

The challenge of applying the Fourth Amendment to modern circumstances, such as when government agents search the cell phone of an arrestee, is best met by applying the terms of the amendment with specificity and care. This Court can provide a sensible rule for cell phone searches and model how to apply the Fourth Amendment for lower courts, by eschewing sweeping pronouncements or guesses about Americans' expectations of privacy. Rather, the Court should apply the terms of the Fourth Amendment to the facts of the case.

---

[1] Pursuant to Rule 37.2(a), all parties were timely notified of and have consented to the filing of this brief. In accordance with Rule 37.6, counsel affirms that no counsel for any party authored any part of this brief and that only *amicus* made a monetary contribution to its preparation or submission.

The Court should analyze distinctly each seizure and search that occurred, closely examining the legal basis for those that are contested. With respect to seizure, use and enjoyment of property are rights distinct from possession that can be seized. Searching a phone makes use of it for the government's purposes, which is a seizure distinct from taking physical possession, and which requires independent legal justification.

The Court should recognize and explicitly state that cell phones are constitutional effects. And it should find that the content stored on cell phones includes constitutional papers and effects distinct from the phones themselves. Digital files stored on cell phones serve the same human ends that papers, postal mail, books, drawings, and portraits did in the founding era.

The searches of petitioner Riley's cell phone did not meet the standards of *Chimel v. California*, 395 U.S. 752 (1969), which allows warrantless searches to protect officers and prevent escape or to prevent destruction of evidence. The methodical application of the Fourth Amendment requires that the judgment of the lower court be reversed.

ARGUMENT

I. THE COURT SHOULD ANALYZE DISTINCTLY EACH SEIZURE AND SEARCH THAT OCCURRED IN THIS CASE

As in many Fourth Amendment cases that this and lower courts consider, the investigation, arrest, and further investigation of petitioner Riley was a series of seizures and searches, some of which are contested. Articulating and distinctly examining

each seizure and search can improve this Court's consideration of the issues, while modeling for lower courts how to apply the Fourth Amendment more precisely in difficult cases. The court below did not articulate well its consideration of the seizure of the cell phone—nor did it articulate the search of the cell phone—which compromised its consideration of the issues.

A. "Seizure" and "Search" Are Distinct Activities, Even if They Are Often Used Together to Investigate Suspects.

This Court's cases have rarely defined "seizure" distinctly from "search." *United States v. Jacobsen*, 466 U.S. 109, 114 n.5 (1984) ("[T]he concept of a 'seizure' of property is not much discussed in our cases"). This is in part because incursions on property rights—seizures—are often the means government agents use to discover information; seizure is the way they search. Often, a seizure or seizures and the search they facilitate have the same legal justification—or they both lack one. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945, 949 (2012) ("The Government physically occupied private property for the purpose of obtaining information."). It is convenient to refer to seizures, especially small ones, and the searches they facilitate collectively as though they are a unitary "search." *See, e.g.*, *Arizona v. Hicks*, 480 U.S. 321, 324 (1987) (moving of stereo equipment to gather serial numbers "constitute[d] a 'search'"). Unfortunately, the convenience of lumping together seizures and searches has occasionally permitted this Court to treat small seizures as though they did not occur. *See, e.g.*, *New York v. Class*, 475 U.S. 106, 114 (1986) (police officer lifting papers not considered a seizure).

Seizures and searches are not the same, and they do not always occur together. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 32 (2001) ("a 'search' despite the absence of trespass"); *Soldal v. Cook County*, 506 U.S. 56 (1992) (seizure of mobile home, not part of search). Collapsing important distinctions between seizure and search can obscure the legal import of government agents' actions—particularly with respect to information technologies, whose Fourth Amendment consequences spring not so much from their possession as from their *use*.

A government agent who only takes possession of a digital device does little to undermine the security of the papers and digital effects its owner has stored on it. A government agent *using* the device to bring stored information out of its natural concealment does a great deal to threaten the interests that the Fourth Amendment was meant to protect.

Casual use of language in a spate of Fourth Amendment cases from the 1980s may suggest that only the "possessory" interest in property can be seized by government agents. *See United States v. Place*, 462 U.S. 696, 705 (1983) (discussing "possessory" interest in luggage); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (seizure found because destruction of powder infringed "possessory interests"); *United States v. Karo*, 468 U.S. 705, 712 (1984) (installation of beeper does not interfere with "possessory" interest); *cf. Karo* 468 U.S. at 729 (Stevens J., dissenting) ("Surely such an invasion is an 'interference' with possessory rights; the right to exclude . . . had been infringed."). In the past, it may have been sound to treat deprivation of "possessory interests" and constitutional "seizures" as one and the same. Nearly always, possession of an item was

the aspect of ownership material to Fourth Amendment cases. This approach does not translate to the information technology context if the interests secured by the Fourth Amendment are to survive.

The right to possess property is one of several aspects of ownership identified in legal philosophy. *See,* TONY HONORÉ, *Ownership, in* OXFORD ESSAYS ON JURISPRUDENCE 104-147 (A.G. Guest ed., 1961). The right to use property is another distinct aspect of ownership. The right to the income of property—the enjoyment of its benefits—is yet another in what law students are taught to be the "bundle of sticks" that comprise property rights.

The Fourth Amendment's proscription on unreasonable seizures is not synonymous with common law trespass, but is both narrower and broader. As an example, the limitation in the Fourth Amendment's text to "persons, houses, papers, and effects" means it does not bar government agents' entry onto open fields with a "no trespassing" sign posted at the border. *Oliver v. United States*, 466 U.S. 170, 176-77 (1984).

"Seizure" also extends beyond common law trespass. Taking possession of persons—which would otherwise constitute the torts of battery and false imprisonment or the crime of kidnapping—is a power government agents enjoy in the proper exercise of their duties. But they may not unreasonably seize people thanks to the Fourth Amendment.

Along with the kinds of things the Fourth Amendment protects from unreasonable seizure, it is important to recognize all the dimensions of seizure, including taking the use and enjoyment of digital devices for the government's benefit. This Court

should recognize that use and enjoyment are property rights that can be seized. Doing so will allow this Court to apply long-standing principles, even in a "high-tech" case, to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34; *Jones*, 132 S.Ct. at 950 (majority opinion); *Id.* at 958 (Alito J., concurring in the judgment).

B. The investigation and arrest of Riley was a series of seizures and searches.

When Officer Dunnigan stopped petitioner Riley, having observed him driving a car with expired registration tags, he seized Riley's car and Riley. *Brendlin v. California*, 551 U.S. 249, 254-263 (2007). Officer Dunnigan had reasonable suspicion that an infraction had occurred, and a brief seizure is permitted in such a case. *Terry v. Ohio*, 392 U.S. 1, 20-27 (1968).

After learning that Riley was driving with a suspended driver's license, Officer Dunnigan removed him from the car and continued the original seizure of Riley with an additional legal basis for doing so: reasonable suspicion of another violation. Officer Dunnigan was then joined by Officer Ruggiero, who prepared the car for impoundment, consistent with a policy that prevents suspended drivers from returning to and continuing to operate their vehicles. No longer seized for the purpose of a brief investigation, the car was now seized in order to prevent additional driving infractions.

As part of the latter, Officer Ruggiero began an "impound inventory search" of the car of the type this this Court approved as reasonable in *South Dakota v.*

Opperman, 428 U.S. 364, 376 (1976).[2] Under new legal authority, Ruggiero commenced a new search.

To be precise, an inventory search of a car is executed through a series of small seizures in addition to, and distinct from, the original seizure of the car as a whole. Officer Ruggiero exercised further dominion over the car by opening the hood, trunk, and other compartments. He exercised additional and particularized dominion over items in the car by picking them up or moving them to facilitate the inventory.

These exercises of dominion over the car and other items touched and moved were all exercises of possession, which is one aspect of ownership. Government agents are allowed to take possession of others' property in the context of a lawful inventory search such as the one that happened here. All these small seizures are part of the "inventory search" and are reasonable under *Opperman*.

Following Officer Ruggiero's discovery of guns in the engine compartment of the car, Officer Dunnigan, having probable cause, placed petitioner Riley under arrest, continuing the initial seizure of Riley under new legal authority. In placing Riley under arrest, Officer Dunnigan also searched his person, undoubtedly doing so by placing his hands on Riley to "seek[] out that which is otherwise concealed

---

[2] The court below noted an investigatory purpose to the search, saying Officer Ruggiero looked under the hood not only because items on the impound sheet are in the engine compartment, but "because he has found contraband under the hood on prior occasions," but it did not investigate the legal propriety of that motivation any further. *People v. Riley* 2013 Cal. App. Unpub. LEXIS 1033 at 9 (2013)

from view"—the definition of "search" from *Black's Law Dictionary*. BLACK'S LAW DICTIONARY 1349 (6th ed. 1990). The search was distinct from the original and ongoing seizure of the body, and its legal basis was different. *Chimel v. California*, 395 U.S. 752, 762-763 (1969), permits a search incident to an arrest to aid in the discovery of weapons or of evidence that could be destroyed.

Consistent with standard practice for a booking search, which is yet another legal basis for searching suspects and seizing property (*see, e.g., Illinois v. Lafayette*, 462 U.S. 640 (1983)), Officer Dunnigan seized Riley's possessions, including his cell phone, for the purpose of transporting and housing his arrestee.

The lower court's description of events is not detailed, but in the process, Dunnigan "looked at Riley's cell phone," and "he noticed all of the entries starting with the letter 'K' were preceded by the letter 'C'." *Riley*, LEXIS 1033 at 8. It is possible that these "entries" were in plain view, displayed by the otherwise untouched phone as Officer Dunnigan seized it. The likelihood is that Dunnigan caused the "entries" to be displayed by manipulating the phone, an additional and separate search. Later at the station, Detective Malinowski, who had come at the request of Officer Dunnigan, "looked through the phone," turning up photos that corroborated evidence suggesting that Riley was involved in gang activity. *Id.*

Officer Dunnigan's apparent search of the phone and Detective Malinowski's clearly described search have similarities to the inventory search of a car.

Both searches were executed through a series of small seizures.

Data in a phone obviously does not decide to display itself. Rather, the phone responds to commands issued by touches and taps on buttons and screens. These touches and taps do not effect possession of the phone, which is already under the complete physical control of the government. Instead, they make *use* of the phone and the data in it to convey stored information to the possessor.

As noted above, *use* is another of the aspects of ownership common to "mature legal systems." HONORÉ, *supra*, at 162, 165. Looking through a phone makes use of the electronics, the battery, the display technology, and the data, none of which are ordinarily the property of the government agent to use. The government agent is allowed to exercise this aspect of ownership—to use the phone as if it were his or her property—with sufficient legal justification. The power of Officer Dunnigan and Detective Malinowski to use the phone this way is what petitioner Riley contests.

Detective Malinowski's seizure of data in downloading it from the cell phone, (Joint App. 14), was an additional step in the process of investigating petitioner Riley. It appears not to be contested, but the legal authority to seize data would spring from discovery of evidence during a lawful search of the cell phone.

The question whether the cell phone search satisfied the Fourth Amendment relies on a premise agreed upon by both parties. This Court should raise and address that premise: the status of cell phones

and their contents as Fourth Amendment "papers and effects."

II. THIS COURT SHOULD RECOGNIZE THAT PHONES ARE THEMSELVES FOURTH AMENDMENT "EFFECTS," AND THAT PHONES CONTAIN FOURTH AMENDMENT PAPERS AND EFFECTS

This Court should explicitly endorse the premise adopted by all parties in this case that a cell phone is an "effect" under the Fourth Amendment. It should also explicitly acknowledge that among other content stored by the cell phone in this case were constitutional "papers and effects."

A. A Cell Phone Is an "Effect" Under the Fourth Amendment.

If a car is an effect for purposes of the Fourth Amendment, *Jones*, 132 S. Ct. at 949, and a footlocker is an effect, *United States v. Chadwick*, 433 U.S. 1, 12 (1977), then a phone must also be an effect. Cell phones are typically carried on one's person. They can contain copious amounts of personal information. They have that "intimate relation" to the person that characterizes personal effects. BLACK'S LAW DICTIONARY 1143 (6th ed. 1990) (defining "personal effects").

Yet *amicus* knows of no case holding that a cell phone is an "effect" for purposes of the Fourth Amendment. Perhaps this is because lower courts treat the matter as too obvious to state, or because Fourth Amendment doctrine leads courts so far from the text of the law, or even because *amicus*'s research skills are inadequate. An explicit holding that a cell phone is an effect would aid the work of courts below—as well as advocates before them—all of

whom might be reminded to think methodically about applying the terms of the Fourth Amendment to the cases they consider.

B. Among Other Content of the Cell Phone Were Constitutional "Papers and Effects."

Cell phones themselves are fairly obviously effects. Some of the contents stored by cell phones are also rightly treated as papers and effects distinct from the material phone. The cell phone government agents seized from Riley contained stored papers and effects, including his photographs. This Court should hold explicitly that the photographs on Riley's cell phone were, for constitutional purposes, papers and effects protected by the Fourth Amendment.

The communications and storage functions of cell phones serve the same human ends today that papers, postal mail, books, drawings, and portraits did in the founding era. This Court should clearly acknowledge that the Fourth Amendment protects digital equivalents of the same types of documents that it protects in analog form.

The Framers used written communications, both public and private, to revolutionize political life on the American continent, so they promptly provided for protection of information against government seizure and search after the founding. Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 559-69 (2007). Congress's first comprehensive postal statute wrote the confidentiality of sealed correspondence into law, with heavy fines for opening or delaying another's mail. *Id* .at 566-57; Act of Feb. 20, 1792, § 16, 1 Stat. 232, 236. This Court

validated Fourth Amendment protection for mail in *Ex Parte Jackson*, 96 U.S. 727 (1877).

Writing on sheets of paper predominated during the founding era, but new ways to store and convey information have emerged since. The invention of Morse Code, for example, allowed words to be transmitted after their conversion into electrical pulses. Lewis Coe, THE TELEGRAPH: A HISTORY OF MORSE'S INVENTION AND ITS PREDECESSORS IN THE UNITED STATES 26-27 (McFarland and Co. 1993). This became relatively common with the emergence of telegraph networks including Western Union in the late 1850s. *Id.* at 86. A new protocol for recording and storing writings was in use.

In the year this Court decided *Ex Parte Jackson*, both Western Union and the Bell Company began establishing voice telephone services. Gerald W. Brock, THE SECOND INFORMATION REVOLUTION 28 (Harvard University Press 2003). Now, instead of messages written on paper carried in the post or telegrams sent along a wire, representations of the human voice itself began moving across great distances. Rather than recording letters and numbers on paper, a microphone in the handset would produce a modulated electrical current that varied its frequency and amplitude in response to the sound waves arriving at its diaphragm. The resulting current was transmitted inaudibly and invisibly along the telephone line to the local exchange, then on to the phone at the other end of the circuit. At its destination, the signal would pass through the coil of the receiver and produce a corresponding movement of the diaphragm in the receiving phone's earpiece. This is the technology this Court confronted in *Olmstead v. United States*, 277 U.S. 438 (1928),

failing to recognize it as a new protocol for communication of the same things that might previously have been contained in a letter.

More recent technological advances have further improved people's ability to record and communicate written words, as well as images and sounds. Digitization—the representation of letters, numbers, symbols, sights, and sounds as 1s and 0s—is a new way of representing the same content as was found in papers, postal mail, books, drawings, and portraits during the founding period.

The federal trial court system has recognized, as it must, that digital representations of information are equivalent to paper documents for purposes of both filing and discovery. *See,* Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, *Report of the Civil Rules Advisory Committee* 2, 18-22, May 27, 2005.[3] The subject matter held in digital documents and communications is at least as extensive and intimate as what is held on paper records, and probably much more so. *See,* Mary Czerwinski et al., *Digital Memories in an Era of Ubiquitous Computing and Abundant Storage*, Communications of the ACM 45, Jan. 2006.[4]

The storage of documents and communications on media other than paper changes nothing about their Fourth Amendment significance. The same information about each American's life that once

---

[3] Available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV5-2005.pdf.

[4] Available at http://research.microsoft.com/pubs/79673/CACMJan2006DigitalMemories.pdf

resided on paper and similar media in attics, garages, workshops, master bedrooms, sewing rooms, and desk drawers (*cf. Chimel*, 395 U.S. at 754), now resides, digitized, in cell phones and similar electronic devices.

Digital representations of information are constitutional "papers and effects" whose security against unreasonable seizure is protected by the Fourth Amendment. It is essential to make clear that the coverage of the Fourth Amendment extends to these media if this Court is to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34

At least one lower court has found constitutional protection for email clearly enough to rely on its premise that email represents a paper or effect.[5] In *United States v. Warshak*, the U.S. Court of Appeals for the Sixth Circuit wrote: "Given the fundamental similarities between email and traditional forms of communications, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail." 631 F.3d 266, 285-6 (6th Cir. 2010).

Email is but one of many protocols that replicate and improve on people's ability to collect, store, and transmit information as they did in the founding era. Images which once had to be drawn, for example, are now commonly digitized using standards like JPEG.

---

[5] Current Fourth Amendment doctrine collapses the existence of a seizure or search and its reasonableness into a single question, whether one's "reasonable expectation of privacy" has been violated. This makes it unclear whether the Sixth Circuit regards email as a paper or an effect.

See, JPEG Homepage, http://www.jpeg.org/jpeg/, (last visited March 9, 2014). There are many protocols that convert text, sound, and images to digital files and permit their transport via modern equivalents of postal mail.

In this case, the Court should find that at the very least the photos discovered by Detective Malinowski and the "entries" discovered by Officer Dunnigan were papers and effects.

Finding that a photo in a cell phone is a constitutional effect does not establish whether its seizure or search is reasonable or unreasonable, constitutional or unconstitutional. These subjects we turn to next.

III. NEITHER SEARCH OF RILEY'S CELL PHONE WAS JUSTIFIED BY THE *CHIMEL* FACTORS

Absent a warrant, the search and seizure of a suspect's property is *"per se* unreasonable" unless justified by one of "a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009). The California Court of Appeals erred in finding that the searches performed by Officer Dunnigan and Detective Malinowski fell into the "search incident to arrest" exception to the warrant requirement, and also in finding that "a delayed search of an item immediately associated with the arrestee's person may be justified as incident to a lawful custodial arrest without consideration as to whether an exigency for the search exists." *Riley*, LEXIS 1033 at 12 (quoting *People v. Diaz*, 244 P.3d 501 (Cal. 2011)).

A. The Exceptions to the Warrant Requirement for Searches Incident to Arrest Do Not Apply to Digital Searches.

This Court did not create a broad new authority for officers to search suspects and seize their property in *Chimel* and *Robinson*. Rather, the Court recognized the continuing validity of two long-standing but separate exceptions to the general rule against warrantless seizures and searches.

In *Chimel*, this Court reiterated the importance of the Fourth Amendment's warrant requirement: "It is a cardinal rule that . . . law enforcement . . . use search warrants wherever reasonably practicable." *Chimel* 395 U.S. at 758 (quoting *Trupiano v. United States*, 334 U.S. 699, 705 (1948)). This Court articulated clearly and sensibly the extent of the "search incident to arrest" principle:

> [I]t is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.

Chimel, 395 U.S. at 763 (1969)

In *United States v. Robinson*, 414 U.S. 218 (1973), this Court further reiterated the two prongs of the "search incident to arrest" exception to the warrant requirement. *Robinson* overturned a ruling suggesting that the only reason for a full search was discovery of evidence or the fruits of a crime. "The

justification or reason for the authority to search incident to a lawful arrest rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial." *Id.* at 234.

The *Robinson* Court pragmatically approved the examination of a crumpled cigarette package on the person of an arrestee, giving rise to a "container" doctrine that this Court has since had to curtail. *See, e.g., Chadwick*, 433 U.S. at 1 (1977); *Arizona v. Gant*, 566 U.S. 332 (2009). Courts have applied this doctrine to cell phones, too—not chastened, apparently, by container-doctrine trends. *See, e.g., People v. Diaz*, 244 P.3d 501 (Cal. 2011); *Hawkins v. Georgia*, 290 Ga. 785, 787 (Ga. 2012); *Massachusetts v. Phifer*, 463 Mass. 790, 795-96 (Mass. 2012).

In retrospect, Justice Marshall's dissent in *Robinson* is prescient. He called for a more granular assessment of the search, saying: "the search in this case divides into three distinct phases: the patdown of respondent's coat pocket; the removal of the unknown object from the pocket; and the opening of the crumpled-up cigarette package." *Robinson*, 414 U.S. at 249-250 (Marshall J., dissenting). He believed that the removal of the cigarette package was unwarranted because the danger was not great and because no evidence of a driving infraction would be found, much less would such evidence be at risk of destruction. *Id.* at 250-255.

That granularity of analysis in Fourth Amendment methodology commends itself to this Court, regardless whether one agrees or disagrees with Justice Marshall's conclusion in *Robinson*. A carefully analytical *Robinson* majority could have

found, for example, that the officer developed reasonable suspicion about the crumpled cigarette pack because there is no good reason to keep one on hand after one's cigarettes are gone.

The "search incident to arrest" doctrine is two separate exceptions to the warrant requirement that enjoy independent pedigrees and rationales. An arresting officer's search for weapons and other dangerous articles has a twofold justification: "[a] due regard for his own safety," *Closson v. Morrison*, 47 N.H. 482, 484 (NH 1867), and the need to prevent the prisoner from escaping custody, which would see "the arrest itself frustrated." *Chimel*, 395 U.S. at 763. Because Riley could not use the digital contents of his phone to attack the arresting officers or to effect his escape, Officer Dunnigan's search was not grounded in "search incident to arrest" principles.

1. Digital Data Is No Threat to Officers.

The average cell phone is fragile, inefficient, and expensive as a bludgeoning tool. But because it could conceivably be used in an attack, its seizure at the time of an arrest is a wise precaution, justified under *Chimel*. Leaving a modern smartphone in an arrestee's possession could aid in his escape—most dramatically by his calling in heavily armed confederates. An arrestee's ability to communicate from detention can also help protect his or her rights, *see, e.g.*, Mallory Simon, *Student 'Twitters' his way out of Egyptian Jail*, CNN.com (2008),[6] but, on balance, in situations with a prospect for violence, taking the phone out of the prisoner's physical reach

---

[6] Available at http://www.cnn.com/2008/TECH/04/25/twitter.buck/index.html

eliminates potential uses in escape and assures officer safety.

But Officer Dunnigan went beyond just confiscating Riley's phone. He used it to reveal digitally stored information—a distinct form of seizure/search that lacked the legal justification of the initial traffic stop, pat-down, and arrest, or the seizure of the phone itself. Looking at Riley's contacts list in no way increased Officer Dunnigan's safety or reduced the likelihood of Riley's escape.

In *Chimel*, this Court permitted the search of areas and objects near a suspect at the time of arrest to ensure officer safety, but limited those searches to areas immediately physically accessible by the suspect, noting that there was no safety justification "for routinely searching any room other than that in which an arrest occurs -- or, for that matter, for searching through all the desk drawers or other closed or concealed areas in that room itself." 395 U.S. at 763. The Court's logic was clear: Even very dangerous weapons like guns and knives pose no risk if the suspect is physically incapable of using them. The necessity of protecting officers during the arrest and transport of prisoners does not justify searching for or seizing weapons that are beyond a prisoner's reach. *See also, Arizona v. Gant*, 556 U.S. 332 (2009) (police may not search a vehicle as a consequence of arresting its driver or owner unless the suspect had physical access to the vehicle at the time of the arrest). Property that cannot be used to cause anyone harm cannot be seized or searched in the name of officer safety.

Detective Malinowski's search of the phone's contents is even less justified. Malinowski did not

take part in Riley's arrest, transfer, or booking (situations in which the *Chimel* exception for officer safety applies), and Riley was not present during Detective Malinowski's search. Malinowski testified that he was not looking for a weapon or threat stored on the phone, but rather evidence of crime: "I went through it looking for evidence, because I know gang members will often video themselves with guns or take pictures of themselves with the guns. I have knowledge. I've seen pictures where guys are arrested with the gun, pictures with them with the firearms on the phone." Joint App. 20.

Neither Officer Dunnigan nor Detective Malinowski had any safety-based reason to be using Riley's phone to search its contents.

2. There was No Threat of Evidence-Destruction.

The other exception to the warrant requirement afforded by *Chimel* and *Robinson* does not permit open-ended searches for any and all incriminating evidence or contraband. Rather, the exception permits search of an arrestee based "on the need to preserve evidence on his person for later use at trial." *Robinson*, 414 U.S. at 234. *See also, Weeks v. United States*, 232 U.S. 383, 392 (1914). When evidence is no longer on an arrestee's person, this branch of "search incident to arrest" doctrine does not apply.

Then-Judge Cardozo tied the scope of this search to ancient English common law traditions, noting that the power to seize a captured criminal's tools and ill-gotten gains "goes back beyond doubt to the days of the hue and cry, when there was short shrift for the thief who was caught 'with the mainour,' still 'in seisin of his crime' (2 Pollock & Maitland History

of English Law, 577, 578). The defendant, conceding the right, would, none the less, restrict the seizure to things subject to be taken under a search warrant when there is no arrest of the possessor." *People v. Chiagles*, 237 N.Y. 193, 196 (N.Y. 1923).

This Court has held that the *Chimel* exception only extends to cases in which seizure alone would be "insufficient" to prevent the evidence's loss or destruction before police could obtain a warrant authorizing a search. *Chadwick*, 433 U.S. at 13. As a general rule, this Court has held that once a physical container, item, or location, is under the exclusive control of law enforcement, the evidence there is "safe" and the police are required to apply for a warrant before conducting a search. *Illinois v. McArthur*, 531 U.S. 326 (2001).

It has been argued that cell phones and other digital devices ought to be treated differently from physical storage containers because of the risk that the suspect's friends, relatives, or co-conspirators would remotely delete the data on the phone. *See, e.g., United States v. Flores-Lopez*, 670 F.3d 803, 807-09 (7th Cir. 2012) ("Other conspirators were involved . . . besides . . . the defendant, and conceivably could have learned of the arrests . . . and wiped the cell phones remotely before the government could obtain and execute a warrant and conduct a search.").

That could be a real prospect in the future, but it was not in this case. There is no evidence that Officer Dunnigan raced to secure the cell phone evidence. He testified that he brought in Detective Malinowski, who was on call, to perform the most invasive search of Riley's phone because of Malinowski's gang

expertise. Dunnigan did not mention any urgency or risk of losing cell phone evidence. (Joint App. 8, 10.)

Phone-wiping is fairly exotic, and in the most common case—a remote signal initiated by the owner—the threat is fairly easily and cheaply defeated either by turning the phone off, removing the battery, or placing the device in a container (commonly known as a "Faraday bag") that shields radio waves. Faraday bags are available for about the same price as a set of handcuffs.

More importantly, this threat is not unique to technological devices. The same threat of evidence destruction can exist in physical environments, but that does not justify warrantless searches of physical property under *Chimel*.

Consider a suspected drug dealer arrested while walking from his car to his place of business. Looking at his key ring, police officers know he has access to at least a residence, a vehicle, a storage unit, and a storefront—and he could be hiding more drugs at any of them. He also has a cell phone, and they think he might have the names and contact information of all his clients and suppliers. If the threat of tampering with the phone data by hypothetical confederates justifies the warrantless search of that phone's digital contents, then the risk that these confederates would go to wherever the drugs are stored and dispose of them likewise justifies warrantless searches of residences, cars, storage units, and businesses to which a suspect has access. The government's argument proves too much.

Warrantless searching of physical property spurred by fear that evidence may be destroyed is governed by this Court's more general exigent

circumstances precedents. *Kentucky v. King*, 131 S.Ct. 1849, 1854 (2011). *See also, Wong Sun v. United States*, 371 U.S. 471 (1963); *Ker v. California*, 374 U.S. 23 (1963); *Welsh v. Wisconsin*, 466 U.S. 740 (1984). *Chimel* does not permit exigent-like searching of a phone when it can be secured while an application for a warrant is made.

There is no legitimate distinction between the risk of hypothetical confederates deleting evidence stored on a phone or in remote storage and their destroying physical evidence when they learn of a co-conspirators arrest. To allow wide-ranging searches on this "confederates" theory would be a sharp departure from the Court's existing view of what is reasonable. The preservation-of-evidence rationale from *Chimel* does not permit police to perform free-standing investigative searches of phones, laptops, and other digital devices.

This Court should not allow government agents to search through a cell phone without a warrant merely because it was properly seized. Doing so would throw open too-wide a door onto suspects' personal and private information without judicial supervision. Cell phones are doorways into people's lives as broad as the front doors of their homes.

Warrantless cell phone searches would also give the government unsupervised access to the personal and private lives of non-suspects. In *United States v. Quintana*, 594 F. Supp. 2d 1291 (M.D. Fla. 2008), for example, a law enforcement officer purportedly investigating the smell of marijuana in a stopped vehicle called the wife of the suspect, then looked through a digital album on the suspect's phone. The album included "photos of an intimate nature"

involving that woman, the suspect's wife, Amy. *Id.* at 1295-96. Whether it is the intimacy of bared breasts, text-based love-notes sprinkled with emoticon hearts ("<3"), or a mother's plea for her wayward, gang-banger son to come home, these are not things for law enforcement officers to rifle through on the streets.

CONCLUSION

Amicus's argument here follows the structure one would use to apply the Fourth Amendment as a law, rather than as a stack of doctrines. Courts should examine whether there was a seizure or search, and whether any such seizure or search was of persons, papers, houses or effects. If those conditions are met, courts should examine whether the warrantless seizures and searches were reasonable.

Using Court-assumed "reasonable expectations" to draw lines around privacy is especially difficult where both technology and societal norms are in flux. "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society becomes clear." *Ontario v. Quon*, 560 U.S. 746, 759 (2010).

Here, well after its seizure, Dunnigan and Malinowski each searched Riley's cell phone, making use of it for their investigative purposes. Because their seizures and searches did not meet *Chimel*'s exceptions to the warrant requirement, they were unreasonable and they violated petitioner Riley's Fourth Amendment rights.

The judgment below should be reversed.

Respectfully submitted,

JIM HARPER
Counsel of Record
ILYA SHAPIRO
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, DC 20001
(202) 842-0200
jharper@cato.org

March 10, 2014

AMICUS CURIAE BRIEF

Supreme Court, U.S.
FILED
MAR 10 2014
OFFICE OF THE CLERK

RECORD
AND
BRIEFS

Nos. 13-132 & 13-212

In the Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

UNITED STATES OF AMERICA,

Petitioner,

v.

BRIMA WURIE

Respondent.

On Writs of Certiorari to the California Court of Appeal, Fourth District and the United States Court of Appeals for the First Circuit

BRIEF OF CENTER FOR DEMOCRACY & TECHNOLOGY AND ELECTRONIC FRONTIER FOUNDATION AS *AMICI CURIAE* IN SUPPORT OF PETITIONER IN NO. 13-132 AND RESPONDENT IN NO. 13-212

EUGENE R. FIDELL
Yale Law School
Supreme Court Clinic
127 Wall St.
New Haven, CT 06511
(203) 432-4992

ANDREW J. PINCUS
Counsel of Record
CHARLES A. ROTHFELD
MICHAEL B. KIMBERLY
PAUL W. HUGHES
Mayer Brown LLP
1999 K Street NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

Library of Congress
Law Library

QUESTION PRESENTED

Amici Curiae will address the following question:

Whether the search-incident-to-arrest doctrine authorizes the government to search—without a warrant and without probable cause—the digitally-stored information contained in a portable electronic device found on the person or within the control of an individual at the time of his or her arrest.

TABLE OF CONTENTS

QUESTION PRESENTED i
TABLE OF AUTHORITIES iv
INTEREST OF THE *AMICI CURIAE* 1
SUMMARY OF ARGUMENT 1
ARGUMENT 4
THE SEARCH INCIDENT TO ARREST DOCTRINE DOES NOT AUTHORIZE WARRANTLESS SEARCHES OF INFORMATION STORED ON AN ELECTRONIC DEVICE. 4
A. Modern Cell Phones And Other Portable Electronic Devices Contain Enormous Amounts Of Sensitive Personal Information That Individuals Formerly Kept In Their Homes. 5
B. The Search-Incident-To-Arrest Exception Does Not Extend To Searches Of Electronically-Stored Data 13
1. The Balance Of Interests Underlying The Exception Does Not Support Blanket Authorization Of Warrantless Searches Of Digitally-Stored Personal Information. 13
2. The Justifications For The Search-Incident-To-Arrest Exception Do Not Apply To Electronically-Stored Data 18
C. The Court Should Reject An Exception To The Warrant Requirement Permitting Searches Of Digitally-Stored Information For Evidence Of The Offense Of Arrest. 26

TABLE OF CONTENTS—continued

D. A Bright-Line Rule Requiring A Warrant For Searches Of Digitally-Stored Information Will Be Much Easier For Officers To Apply Than Other Proposed Standards. 29

1. There Are No Clear Distinctions Between "Smart" And "Dumb" Cell Phones. 30

2. Permitting Law Enforcement Officers To Access Only Certain Types Of Digitally-Stored Information Is Wholly Impractical. 31

3. Distinguishing Between Searches At The Place Of Arrest And Searches At The Police Station Would Increase The Intrusion On Privacy Interests Protected By The Fourth Amendment. 34

CONCLUSION 35

TABLE OF AUTHORITIES

Cases

Arizona v. *Gant*,
556 U.S. 332 (2009) ..... *passim*

Arizona v. *Hicks*,
480 U.S. 321 (1987) 24

Brigham City v. *Stuart*,
547 U.S. 398 (2006) 23

California v. *Acevedo*,
500 U.S. 565 (1991) 21

Chimel v. *California*,
395 U.S. 752 (1969) ..... *passim*

City of Ontario v. *Quon*,
560 U.S. 746 (2010) 1, 4

Cupp v. *Murphy*,
412 U.S. 291 (1973) 23

Dunaway v. *New York*,
442 U.S. 200 (1979) 29

Florida v. *Wells*,
495 U.S. 1 (1990) 25

Illinois v. *Lafayette*,
462 U.S. 640 (1983) 25

Illinois v. *McArthur*,
531 U.S. 326 (2001) 23

Katz v. *United States*,
389 U.S. 347 (1967) 4

Kyllo v. *United States*,
533 U.S. 27 (2001) 4, 17, 33

Maryland v. *King*,
133 S. Ct. 1958 (2013) 17, 18

Michigan v. *Summers*,
452 U.S. 692 (1981) 29

TABLE OF AUTHORITIES—continued

Mincey v. *Arizona*,
437 U.S. 385 (1978) 23

Missouri v. *McNeely*,
133 S. Ct. 1552 (2013) 4, 23, 28, 30

Thornton v. *United States*,
541 U.S. 615 (2004) 27

United States v. *Chadwick*,
433 U.S. 1 (1977) 21, 22

United States v. *Davis*,
787 F. Supp. 2d 1165 (D. Or. 2011) 25

United States v. *Edwards*,
415 U.S. 800 (1974) 34

United States v. *Flores*,
122 F. Supp. 2d 491 (S.D.N.Y. 2000) 25

United States v. *Jones*,
132 S. Ct. 945 (2012) ..... *passim*

United States v. *Rabinowitz*,
339 U.S. 56 (1950) 27

United States v. *Robinson*,
414 U.S. 218 (1973) 18, 19

United States v. *Wall*,
08-60016-CR, 2008 WL 5381412
(S.D. Fla. Dec. 22, 2008) 25, 26

Virginia v. *Moore*,
553 U.S. 164 (2008) 14

Weeks v. *United States*,
232 U.S. 383 (1914) 14, 15

Other Authorities

128GB phone now available from Meizu, but only works in China, Engadget (Nov. 18, 2013), http://perma.cc/SN77-V24S 8

TABLE OF AUTHORITIES—continued

James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, The Guardian (Jan. 28, 2014, 2:51 AM), http://perma.cc/3LKY-YDWR 32

Charles Arthur, *iPhone keeps record of everywhere you go*, The Guardian (Apr. 20, 2011), http://perma.cc/S6LC-4UN8 12

Christopher Barnatt, *A Guide to Computing: Mobile Computing* (Nov. 2, 2013), http://perma.cc/TWU9-VVTZ 5

Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart, ACLU, http://perma.cc/J2R7-9N6B. 12

Compare iPad Electronic Medical Records Software, Software Advice, http://perma.cc/K3FH-DJLY 11

Conner Technical Services, http://perma.cc/QN3L-XT8R 5

Consumer Electronics, 2013 WLNR 27310700 (Oct. 28, 2013) 6

Definition of: feature phone, PC Magazine Encyclopedia, http://perma.cc/6RHP-DKRG 7

Definition of: Smartphone, PC Magazine Encyclopedia, http://perma.cc/647Z-MGRW 7

Design Principles, Android Developer, http://perma.cc/N534-576H 33

Does Foursquare track my location?, Foursquare Help Center, http://perma.cc/U63C-CHNM. 12

TABLE OF AUTHORITIES—continued

Jill Duffy, *Best Mobile Finance Apps*, PC Magazine (Oct. 8, 2013), http://perma.cc/QS9Y-TQT4. 11

Derek Fung, *What Storage Should I Get in My Camcorder?* , CNET Australia (Sept. 23, 2009), http://perma.cc/QHX9-KNQ6 8

Samuel Gibbs, *Apple's iWatch: What Features Are on Our Wishlist?*, The Guardian (Feb. 4, 2014, 5:14 PM), http://perma.cc/A4V6-D6WN 13

How Much Does a Ream of Paper Weigh?, Ask.com, http://perma.cc/7WQ5-2HCB 15

How much data is there on a hard drive?, Ctr. for Computer Forensics, http://perma.cc/T6CL-JTHG 8

iOS Human Interface Guidelines 62 (2014), http://perma.cc/M5DA-24DR 33

Richard Lai, *World's first 128GB phone now available from Meizu, but only works in China*, Engadget (Nov. 18, 2013), http://perma.cc/SN77-V24S 8

Rob LeFebvre, *New App For People With Alzheimer's Launches Today, Free For Limited Time*, Cult of Mac (Aug. 19, 2013, 11:00 AM), http://perma.cc/QS9Y-TQT4 11

Stephanie Mlot, '*Premium' Nokia 515 Feature Phone Unveiled*, P.C. Magazine (Aug. 28, 2013, 4:06 PM), http://perma.cc/N3ZJ-C8SQ 30

James Madison Papers, Library of Congress, http://perma.cc/LPS5-45NG 15

TABLE OF AUTHORITIES—continued

Megabytes, Gigabytes, Terabytes ... What Are They?, What's a Byte, http://perma.cc/8AAW-MVZQ 8

Claire Cain Miller, *Google Glass to Be Covered by Vision Care Insurer VSP*, N.Y. Times (Jan. 28, 2014) 13

National Heart, Lung, and Blood Inst., http://perma.cc/4UCA-XEQB 13

Alexei Oreskovic, *Google's new Gmail feature linking social network contacts raises privacy concerns*, Financial Post (Jan. 10, 2014, 11:56 AM), http://perma.cc/QL5U-MVM3 10

Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. Times (Feb. 15, 2012, 9:05 AM) 31

PC Magazine (Oct. 8, 2013), http://perma.cc/QS9Y-TQT4 11

PC Magazine Encyclopedia, http://perma.cc/647Z-MGRW 7

PC Magazine Encyclopedia, http://perma.cc/6RHP-DKRG 7

Pew Research Center, *Cell phone ownership hits 91% of adults* (June 6, 2013), http://perma.cc/ALM7-QZBJ 7

SanDisk Ultra 16 GB, Amazon.com, http://perma.cc/ALS6-SU9F 6

Shane Cole, *Apple's iPhone 5s remains 'by far the top selling smartphone,'* Apple Insider , http://perma.cc/PP3W-XQZV 7

Smokefree Apps, Smokefree.gov, http://perma.cc/4QBP-8DZR 11

TABLE OF AUTHORITIES—continued

Software Advice, http://perma.cc/K3FH-DJLY 11

Somak R. Das et al., *Home Automation and Security for Mobile Devices*. 2011 33

Staples Advantage, http://perma.cc/AAG7-H566 6

Statistical Trends & Numbers (Aug. 12, 2012), http://perma.cc/9PFX-DPEE 7

Tablet: What is it? Which Tablet is Right for Me?, Staples Advantage, http://perma.cc/AAG7-H566 6

The 13 Best Diabetes iPhone & Android Apps of 2013, Healthline (Aug. 8, 2013), http://perma.cc/UPY9-EGTS 11

The Amazing History of Information Storage: How Small Has Become Beautiful, Statistical Trends & Numbers (Aug. 12, 2012), http://perma.cc/9PFX-DPEE 7

TracFone LG440G Cell Phone, Walmart, http://perma.cc/RDR2-JCLY 30

Trends shaping mobile forensics in 2014, http://perma.cc/R8EA-GBP2 34

USB Flash Drives: How Much Storage Space is Enough?, eBay, http://perma.cc/D4MQ-HV8X 6

What Is a Pacemaker?, National Heart, Lung, and Blood Inst., http://perma.cc/4UCA-XEQB 13

INTEREST OF THE *AMICI CURIAE*

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing civil liberties issues raised by emerging technologies.

CDT and EFF have participated as *amici* in cases before this Court involving the application of the Fourth Amendment to new technologies, including *City of Ontario* v. *Quon*, 560 U.S. 746 (2010), and *United States* v. *Jones*, 132 S. Ct. 945 (2012).[1]

SUMMARY OF ARGUMENT

Modern cell phones and other portable electronic devices contain very large amounts of sensitive, personal information—including an archive of communications with family and close friends, the equiva-

---

[1] Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici* and their counsel made a monetary contribution to its preparation or submission. The parties' letters consenting to the filing of this brief have been filed with the Clerk's office.

lent of bookshelves worth of photo albums, and substantial personal medical and financial information.

Prior to the advent of digital technology, this information would have been stored in the drawers and file cabinets of people's homes. Law enforcement officers would have been required to obtain a warrant in order to search such materials.

The question before the Court is how the Fourth Amendment applies in light of this significant advance in technology—in particular, whether the search-incident-to-arrest exception authorizes warrantless searches of all of the information stored digitally on a portable electronic device found on an arrested individual's person.

Permitting warrantless searches of this large amount of information is inconsistent with the Fourth Amendment for three reasons.

First, the search-incident-to-arrest exception was recognized in the earliest days of our Nation, when information could be transported only if it was written on paper. That reality imposed a significant inherent limitation on the scope of the exception: because the amount of information an individual could carry was restricted by the weight and bulk of paper, the exception's intrusion on sensitive personal information would be circumscribed.

Technology now makes it possible for individuals to carry huge quantities of information with them every day. Permitting warrantless searches of digitally-stored information will allow police to rummage through vast quantities of individuals' personal information—precisely what the Framers of the Fourth Amendment sought to prevent.

Second, neither of the justifications for the exception support a search of the data stored on an electronic device. An inspection of the device is sufficient to establish that it poses no threat to police officers. And once the police officer has seized the device there is no risk that the arrestee himself will be able to access the device and destroy evidence. If the risk of destruction of evidence is present in a particular case—because the officers reasonably believe that the particular device's digitally-stored information will be deleted by the actions of a third party or other means that they cannot prevent using reasonably-available countermeasures—the well-established exigent circumstances exception will allow officers to act to preserve the information (but not search it) without obtaining a warrant.

Third, a bright-line rule requiring police officers to obtain a warrant before searching digitally-stored information is clear and therefore easily administrable. Standards under which the need for a warrant would turn on the relative sophistication of the particular portable electronic device would be impossible for officers to apply—they could not possibly keep track of the various relative capabilities of the myriad different types and models of these devices. Similarly, a rule that allows officers to search some categories of information but not others makes no sense because these devices increasingly are designed to integrate the different categories of information stored on the device and to seamlessly access remotely-stored data in ways that make it indistinguishable form the data stored on the device.

Finally, the warrant requirement is not burdensome. Once police have seized the device, it will not be difficult to present the warrant request to a judi-

cial officer and, if probable cause is shown, obtain the authorization that the Fourth Amendment requires.

ARGUMENT

THE SEARCH INCIDENT TO ARREST DOCTRINE DOES NOT AUTHORIZE WARRANTLESS SEARCHES OF INFORMATION STORED ON AN ELECTRONIC DEVICE.

This Court has recognized repeatedly that the Fourth Amendment's protections against government intrusions must be construed in light of the nature and effects of advances in technology. *United States* v. *Jones*, 132 S. Ct. 945 (2012); *City of Ontario* v. *Quon*, 560 U.S. 746 (2010); *Kyllo* v. *United States*, 533 U.S. 27 (2001).

When new technologies would allow the government to access previously unavailable information, the Court has taken those developments into account in delineating the Fourth Amendment's protections. See, *e.g.*, *Jones*, *supra* (GPS tracking device); *Kyllo*, *supra* (thermal imaging device); *Katz* v. *United States*, 389 U.S. 347 (1967) (wiretap of payphone); cf. *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1562-1563 (2013) (acknowledging that "technological developments that enable police officers to secure warrants more quickly * * * are relevant to an assessment of exigency").

That same need to consider the impact of advances in technology is presented in these cases as a result of innovations permitting digital storage of large amounts of information on increasingly ubiquitous portable electronic devices. Although the searches here involved information stored on cell phones, the federal government recognized below that its legal theory is not limited to those particular

devices and would permit the search of all digitally-stored data on "any electronic device seized from a person during his lawful arrest, including a laptop computer or a tablet device such as an iPad." 13-212 Pet. App. 15a.

A. Modern Cell Phones And Other Portable Electronic Devices Contain Enormous Amounts Of Sensitive Personal Information That Individuals Formerly Kept In Their Homes.

Advances in digital technology permit the storage on portable electronic devices of huge amounts of personal information—including communications with family and friends, diaries, pictures, and financial and health records—that individuals typically kept in their homes before the digital era. This information is generated in substantial part as a result of innovations that permit the use of these portable devices to send and receive email and text messages, and to perform a myriad of other functions.

The two cases before the Court involve cell phones, but many different types of portable electronic devices have the information-storage and other characteristics of cell phones.[2] For example, tablet computers and laptop computers have extensive storage, computing, and communication features.[3]

---

[2] All of these devices, like cell phones, store data electronically in a series of *1*'s and *0*'s. Conner Technical Services, http://perma.cc/QN3L-XT8R) ("The only [numbering system] * * * that an electronic device uses is binary * * * *.").

[3] Christopher Barnatt, *A Guide to Computing: Mobile Computing* (Nov. 2, 2013), http://perma.cc/TWU9-VVTZ (explaining that modern laptops have the same functionality as desktop computers). Modern tablets allow a user to "browse the inter-

Digital cameras have substantial storage capabilities—for both still pictures and video, including sound.[4] And "thumb drives," small devices no larger than a thumb, can also store huge quantities of data.[5]

Thus, although we focus below on the capabilities of modern cell phones, those capabilities are shared by a significant number of other portable electronic devices that individuals routinely carry on their persons. And the variety of such devices is growing significantly as innovators find new ways to use electronic communications, storage, and computing technologies.

Modern cell phones[6] are ubiquitous: 91% of American adults own one.[7] These devices have dra-

---

net, create and share presentations, video[] conference with clients, stay connected with corporate email, download books, games and videos, watch movies, share photos and much more * * * ." *Tablet: What is it? Which Tablet is Right for Me?*, Staples Advantage, http://perma.cc/AAG7-H566.

[4] The basic storage medium for images and video on a digital camera—flash memory—sells for $12 at 16 GB, which can hold 8,000 images or one hour of high-resolution video with sound. See *SanDisk Ultra 16 GB*, Amazon.com, http://perma.cc/ALS6-SU9F. Recently released memory cards for cameras already store up to four times more data than today's cell phones. See Consumer Electronics, 2013 WLNR 27310700 (Oct. 28, 2013) (noting that SanDisk released a 256 gigabyte memory card to keep up with developments in photography and videography).

[5] Even a small and simple thumb drive, which holds 2 GB of data and sells for less than four dollars at Walmart, see http://perma.cc/YZD5-MCFX, can hold up to one thousand photographs, *USB Flash Drives: How Much Storage Space is Enough?*, eBay, http://perma.cc/D4MQ-HV8X.

[6] Modern cell phones are sometimes described using two general, and overlapping, terms—"feature phone" and "smartphone." A smartphone is "[a] cellular telephone with built-in

matically expanded the amount and types of information that Americans carry every day.

The amounts of information that these devices can contain are staggering. For example:

- The Apple iPhone 5 is the largest-selling smartphone;[8] the version with the smallest storage capability (16 gigabytes ("GB")) can store 800 million words of text[9]—well over a

---

applications and Internet access. In addition to digital voice service, modern smartphones provide text messaging, e-mail, Web browsing, still and video cameras, MP3 player and video playback and calling." *Definition of: Smartphone*, PC Magazine Encyclopedia, http://perma.cc/647Z-MGRW. Feature phones usually contain "a fixed set of functions beyond voice calling and text messaging, but [are] not as extensive as a smartphone." *Definition of: feature phone*, PC Magazine Encyclopedia, http://perma.cc/6RHP-DKRG. Thus, both types of phones store data digitally, and both provide text messaging and some common additional features, with smartphones providing a wider array of such features. We use "modern cell phones" to refer to both categories, unless specifically noted otherwise.

[7] Pew Research Center, *Cell phone ownership hits 91% of adults* (June 6, 2013), http://perma.cc/ALM7-QZBJ ("[T]he cell phone is the most quickly adopted consumer technology in the history of the world.").

[8] See Shane Cole, *Apple's iPhone 5s remains 'by far the top selling smartphone,'* Apple Insider (Dec. 12, 2013, 8:06 AM), http://perma.cc/PP3W-XQZV.

[9] *The Amazing History of Information Storage: How Small Has Become Beautiful*, Statistical Trends & Numbers (Aug. 12, 2012), http://perma.cc/9PFX-DPEE (noting that the complete 2010 Encyclopedia Britannica, which contains 32 volumes, weighs 129 pounds in physical form, and contains 50 million words, could fit in a single gigabyte of data).

football field's length of books[10] or, to use another measure, sixteen flat-bed truckloads of paper.[11]

- The same phone can contain over 8,000 digital pictures,[12] over 260,000 private voicemails,[13] or hundreds of home videos.[14]
- Other versions of the iPhone, with 32 GB or 64 GB of storage capacity, would be able to store twice or four times those amounts. Some manufacturers have produced phones with 128 GB memory—and therefore the ability to store *eight times* the amount of information contained on a 16 GB phone.[15]

These examples describe the storage capacity of modern cell phones in terms of "books," "photo-

---

[10] An American football field, including end zones, is 120 yards long. Since "1 Gigabyte could hold the contents of about 10 yards of books on a shelf," 16 GB would correspond to about 160 yards of books. *Megabytes, Gigabytes, Terabytes ... What Are They?*, What's a Byte, http://perma.cc/8AAW-MVZQ.

[11] *How much data is there on a hard drive?*, Ctr. for Computer Forensics, http://perma.cc/T6CL-JTHG.

[12] *Number of pictures that can be stored on a memory device*, SanDisk, http://perma.cc/J7JW-7AC7.

[13] Assuming each voicemail lasts thirty seconds and is recorded at a bitrate of 16 kbps, a 16 GB device could hold over 266,666 voicemails.

[14] Assuming each home video is thirty seconds long, recorded at standard definition, 16 GB could store 480 such videos. See Derek Fung, *What Storage Should I Get in My Camcorder?*, CNET Australia (Sept. 23, 2009), http://perma.cc/QHX9-KNQ6.

[15] See Richard Lai, *World's first 128GB phone now available from Meizu, but only works in China*, Engadget (Nov. 18, 2013), http://perma.cc/SN77-V24S.

graphs," "videos," and "voicemails" for ease of explanation, but the information is stored on these devices in many different forms—including text messages, e-mails, Internet browsing records, documents, diary entries, "to do" lists, and sound recordings, as well as books, photographs and videos. And they typically include individuals' most personal information in each of these categories.

First, messages to or from family and close friends are often memorialized as emails, text messages, or voicemail messages. The user's own personal thoughts are contained in an electronic diary or notes or other documents. Photographs and video recordings capture an individual's most personal moments.

These devices' extensive storage capacity means that they do not contain messages, personal thoughts, or photographs and videos from only the last several days, or only the last several weeks. Rather, they can and frequently do retain this information from prior months or even years.

Before the development of portable devices with extensive digital storage capability, of course, it would have been impossible for anyone routinely to carry on his or her person more than a few days' worth of these materials. The vast majority of the information that today is stored digitally on these devices would have been stored in the individual's home or office.

Second, electronic appointment calendars on cell phones store sensitive information about a user's daily activities—including appointments with doctors of all types, religious advisors, psychiatrists, therapists, drug or alcohol-treatment groups, grief counselors,

political groups, marital counselors, and fertility consultants, among many others. And, because these calendars preserve past appointments, they provide a detailed, multi-year record of the user's activities—something that individuals would not ordinarily carry every day before the invention of these devices.

Third, modern cell phones also list the telephone calls made from or received by the phone, but typically integrate that data with other information stored on the phone. That integration function often provides the name, address, and other information regarding the individual associated with the particular phone number, such as his or her relationship to the cell phone's owner.[16]

Fourth, the ability of modern cell phones to function as computers—with an incredibly varied capabilities provided by software programs called "applications" or "apps"—means that these devices often perform functions that result in the storage on the device of additional types of information.

Thus, Electronic Health Record (EHR) "apps" are widely available for smartphones; they are used by both medical professionals and patients to keep track of private medical information in electronic form.[17] Other medical information apps include diabetes

---

[16] Google's popular Gmail email service, for instance, is linked to its "Contacts" address book feature, which is also linked to its Google+ social network feature. See Alexei Oreskovic, *Google's new Gmail feature linking social network contacts raises privacy concerns*, Financial Post (Jan. 10, 2014, 11:56 AM), http://perma.cc/QL5U-MVM3.

[17] See, *e.g.*, *Compare iPad Electronic Medical Records Software*, Software Advice, http://perma.cc/K3FH-DJLY.

tracking apps,[18] apps to help smokers quit,[19] and Alzheimer's disease apps.[20] These apps result in the storage on the cell phone of users' most intimate medical information.

Personal finance apps cause the storage on the cell phone of similarly sensitive financial information, because they link to bank accounts, keep track of investments, and catalog assets. These apps "extract real-time data from your service providers—including banks, investment houses, lenders, and credit card companies," replacing "the pre-PC days when tracking your expenses involved saving receipts, writing down transactions, [and] opening paper bills."[21]

Again, prior to the development of these storage, communication, and computing technologies, individuals would not carry this information with them every day. Sensitive financial and medical information would be kept at home or in the office, with selected physical documents placed in a purse or briefcase only if needed for a particular purpose on a particular day.

Fifth, many modern cell phones routinely use Global-Positioning-System ("GPS") data to determine

---

[18] See, *e.g.*, *The 13 Best Diabetes iPhone & Android Apps of 2013*, Healthline (Aug. 8, 2013), http://perma.cc/UPY9-EGTS.

[19] See, *e.g.*, *Smokefree Apps*, Smokefree.gov, http://perma.cc/4QBP-8DZR.

[20] See, *e.g.*, Rob LeFebvre, *New App For People With Alzheimer's Launches Today, Free For Limited Time*, Cult of Mac (Aug. 19, 2013, 11:00 AM), http://perma.cc/QS9Y-TQT4.

[21] Jill Duffy, *Best Mobile Finance Apps*, PC Magazine (Oct. 8, 2013), http://perma.cc/QS9Y-TQT4.

the phone's location whenever the phone is turned on—because location information is used in many apps.[22] That GPS data is archived, providing a record of the user's movements any time the phone is turned on.[23] The highly personal nature of this information was recognized by the Court in *United States* v. *Jones*. See 132 S. Ct. at 963-964 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment); *id.* at 955-956 (Sotomayor, J., concurring).

Moreover, technology is continuing to evolve. New devices such as smart watches and Google Glass will increase the types and amounts of electronically-stored personal information that individuals carry with them each day. Thus, "[a] smartwatch packed with sensors designed to provide body monitoring information could enable many fascinating new data-driven applications, from fitness tracking to mood-linked music commanded by your heartbeat. * * * Apple holds patents for sensory information collection, including blood-pressure monitoring."[24]

---

[22] For example, the popular application Foursquare "use[s] the location information from your mobile device to tailor the Foursquare experience to your current location." *Does Foursquare track my location?*, Foursquare Help Center, http://perma.cc/U63C-CHNM.

[23] See Charles Arthur, *iPhone keeps record of everywhere you go*, The Guardian (Apr. 20, 2011), http://perma.cc/S6LC-4UN8. Moreover, cell phone companies also store location data for extended periods, often years. *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, http://perma.cc/J2R7-9N6B.

[24] Samuel Gibbs, *Apple's iWatch: What Features Are on Our Wishlist?*, The Guardian (Feb. 4, 2014, 5:14 PM), http://perma.cc/A4V6-D6WN.

Similarly, "Google Glass, the Internet-connected eyewear" could "lead to a world in which people wear or even ingest computers" that monitor and store a wide variety of individuals' personal medical information.[25]

B. The Search-Incident-To-Arrest Exception Does Not Extend To Searches Of Electronically-Stored Data.

The search-incident-to-arrest doctrine is an exception to the Fourth Amendment's generally-applicable requirements of a warrant and probable cause. Given the significant privacy interests at stake, law enforcement officers must obtain a warrant to search digitally-stored data on cell phones and other portable electronic devices.

1. *The Balance Of Interests Underlying The Exception Does Not Support Blanket Authorization Of Warrantless Searches Of Digitally-Stored Personal Information.*

"In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." *Jones*, 132 S. Ct. at 963 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment). That is particularly true of the search-incident-to-arrest exception.

The exception has deep roots. A century ago this Court stated that it was "always recognized under

---

[25] Claire Cain Miller, *Google Glass to Be Covered by Vision Care Insurer VSP*, N.Y. Times (Jan. 28, 2014), http://perma.cc/H6AR-96YG. Indeed, digital devices such as pacemakers already installed in the human body can store data such as one's heart rate and breathing rate. *What Is a Pacemaker?*, National Heart, Lung, and Blood Inst., http://perma.cc/4UCA-XEQB.

English and American law." *Weeks* v. *United States*, 232 U.S. 383, 392 (1914); see also *Virginia* v. *Moore*, 553 U.S. 164, 170 (2008) ("[S]earches incident to warrantless arrests * * * were * * * taken for granted at the founding.") (quotation marks omitted).

At that time, the amount of personal information that an arrestee could carry on his person or have within his control was quite limited. Information could be carried only in physical form—as papers (and later as photographs).

Because of that physical limitation, individuals typically carried with them only the documents needed for that day's activities, plus whatever else might be useful provided that it would fit in a wallet, address book, or briefcase or purse. Individuals did not (and could not) routinely carry large amounts of personal correspondence, photograph albums (or painted family portraits), financial records, or other private information. That information was stored in the individual's home or office.

From the time of its creation until very recently, therefore, the exception had a built-in limitation: the amount of paper that an individual could carry on his or her person or have within his or her reach at the time of arrest. See *Chimel* v. *California*, 395 U.S. 752, 763 (1969) (holding that a search incident to arrest encompasses the arrestee's person and space "within his immediate control").

That physical reality, and the exception's resulting inherent limitation, explains why the search-incident-to-arrest exception was fully compatible with the Founders' determination to prohibit the general warrants and writs of assistance authorizing indiscriminate searches. See, *e.g.*, *Chimel*, 395 U.S.

at 761; *Weeks*, 232 U.S. at 390 (discussing the Fourth Amendment's origin). Because individuals did not routinely carry all, most, or even many of their private papers with them each day, there was no danger that the exception would be abused to permit rummaging through an individual's most private papers—those papers were safely at home, where, even after the homeowner's arrest, a warrant would be required to search them.

Modern technology has fundamentally changed the amount and nature of the personal information that an individual typically carries and has within his or her reach.

To take one example, the Library of Congress's collection of James Madison's papers consists of approximately 72,000 pages of documents.[26] Madison did not and could not carry those documents on his person—they would have weighed at least 675 pounds.[27] They were kept in his home and in the homes of his correspondents.

Today, however, a cell phone can contain more than 100 times the number of pages in the entire Madison collection.[28] Digital data storage makes it possible for Americans to carry with them every day vast quantities of sensitive information that previously was kept within their homes. See pages 5-13,

---

[26] See *James Madison Papers*, Library of Congress, http://perma.cc/LPS5-45NG.

[27] *How Much Does a Ream of Paper Weigh?*, Ask.com, http://perma.cc/7WQ5-2HCB (noting that a ream of paper weighs approximately 4.7 pounds).

[28] Assuming 400 words per page, a 16 GB iPhone can hold 800 million words, or 2 million pages. See note 9, *supra*. A 64 GB iPhone can hold 8 million pages.

supra. Moreover, the breadth of that information would likely reveal an individual's medical history, religious beliefs, political affiliations, network of friends, colleagues, intimate associates, and acquaintances.

Allowing law enforcement officers to conduct warrantless searches of this electronically-stored information therefore cannot be justified based on precedents that necessarily rest on the much narrower intrusion on privacy interests that could possibly have resulted from searches-incident-to-arrest of physical, rather than digital, materials. Given the dramatically broader intrusion that would result from a blanket authorization of warrantless searches of all digitally-stored information—akin to the significant intrusion that the Fourth Amendment was intended to prevent—those precedents cannot support extension of the exception into this new context.

Indeed, the United States' mechanical invocation of precedent divorced from context here closely resembles the argument that the government advanced—and a majority of the Court rejected—in *United States* v. *Jones*. There, the government argued that precedents finding no reasonable expectation of privacy in an individual's movements on public streets, because of police officers' ability to observe those movements, meant that GPS tracking did not constitute a Fourth Amendment search.

A majority of the Court rejected that argument. 132 S. Ct. at 964 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment) (finding a Fourth Amendment search because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and

catalogue every single movement of an individual's car for a very long period"); *id.* at 956 (Sotomayor, J., concurring) (recognizing that the "attributes of GPS monitoring" must be taken "into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements"); see also *Kyllo*, 533 U.S. at 34 (refusing to "permit police technology to erode the privacy guaranteed by the Fourth Amendment").

Fourth Amendment search-incident-to-arrest decisions that rest upon completely inapplicable assumptions should be held inapplicable here for the same reason. New technology permits a very substantial intrusion on core Fourth Amendment interests that was not anticipated, and could not have been anticipated, when the search-incident-to-arrest exception was recognized.

The federal government argues that the doctrine is nonetheless applicable, repeatedly referencing "the reduced expectations of privacy triggered by the fact of arrest." No. 13-212 U.S. Br. 19. This Court, however, has rejected the notion that "any search is acceptable solely because a person is in custody. Some searches, such as invasive surgery, or a search of the arrestee's home, involve either greater intrusions or higher expectations of privacy." *Maryland* v. *King*, 133 S. Ct. 1958, 1979 (2013) (internal citations omitted). If "the privacy-related concerns are weighty enough * * * the search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Ibid.*

Here, the intrusion on privacy interests from routine searches of digitally-stored information would be very substantial, because of the large amounts of personal information stored on portable

electronic devices. And, as we next discuss, neither the law enforcement interests underlying the search-incident-to-arrest exception nor other law enforcement interests come close to justifying warrantless searches of this information.

2. The Justifications For The Search-Incident-To-Arrest Exception Do Not Apply To Electronically-Stored Data.

In *Chimel* v. *California*, 395 U.S. 752 (1969), the Court explained the "analysis [that] underlies the 'search incident to arrest' principle, and marks its proper extent." *Id.* at 762; accord *Arizona* v. *Gant*, 556 U.S. 332, 343 (2009) (refusing to "untether" the exception from *Chimel*'s justifications).

The federal government argues that *Chimel* is irrelevant, because the Court's decision in *United States* v. *Robinson*, 414 U.S. 218 (1973), recognizes plenary authority to search any object found on the arrestee's person. See No. 13-212 U.S. Br. 17-28. That contention is wrong for two reasons.

To begin with, it ignores the fundamentally different question presented by application of the search-incident-to-arrest exception to digitally-stored information. For the reasons discussed above, any such blanket rule should not be extended to this extremely different context.

But the government's argument is also wrong on its own terms. *Robinson*'s focus was the lower court's narrow view of a police officer's authority to search an arrestee—the court of appeals had held that the officer "may not ordinarily proceed to fully search the prisoner" but could only "conduct a limited frisk of the outer clothing and remove such weapons that he may, as a result of that limited frisk, reasonably be-

lieve and ascertain that the suspect has in his possession." 414 U.S. at 227.

This Court squarely rejected that conclusion, holding that "in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment." *Id.* at 235. That holding says nothing about searches of objects found on the arrestee's person.

Only one sentence of the *Robinson* opinion addressed that question. The Court stated: "Having in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it; and when his inspection revealed the heroin capsules, he was entitled to seize them * * *." *Id.* at 236.

The Court did not explain why the officer was "entitled to inspect" the package. Most likely, it was because, as the government itself argued in *Robinson*, that further search was justified to determine that the package did not contain a weapon. See No.13-132 Pet. Br. 18 (discussing government's argument).

But the Court's unexplained conclusory statement certainly provides no basis for transforming *Robinson*'s holding—that officers may conduct a full search of the arrestee's person—into authority for officers to conduct a full search of everything found on his person, even if *Chimel*'s justifications do not apply.

That is especially true because, as the government acknowledges, the officers' ability to search without a warrant objects not found on the arrestee's person does turn on whether those justifications are

present. No. 13-212 U.S. Br. 21-23. In the government's view, therefore, it may download the full contents of a cell phone without a warrant if the phone is in the arrestee's pocket, but it may not do so if the phone is on the seat next to him. Given the very substantial amount of personal information involved, it is nonsensical for the warrant requirement to turn on such a distinction.

The question in both situations is whether the *Chimel* justifications for the search-incident-to-arrest exception apply. And neither of the two rationales identified in *Chimel* permits searches of the electronically-stored contents of a cell phone.

First, the exception rests on the determination that "it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape." *Chimel*, 395 U.S. at 763. Removal of the mobile phone from the arrestee's possession and examination by the officers to ensure that it is not a disguised weapon (and that it cannot be used by the arrestee to summon his confederates) are all that is necessary to fulfill that purpose.

Second, "it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." *Id.* at 763. The sole concern is the risk of concealment or destruction of evidence *by the arrestee*. *Chimel* explained that the justification extends to a search of "the area 'within his immediate control'—construing that phrase to mean the area from within which [the arrestee] might gain possession of * * * destructible evidence." *Ibid.*

That is why "the *Chimel* rationale authorizes police to search a vehicle incident to a recent occupant's arrest *only when* the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." *Gant*, 556 U.S. at 343 (emphasis added); see also *United States* v. *Chadwick*, 433 U.S. 1, 15 (1977) (stating that once the officers had "exclusive control," "there [was] no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence"), abrogated on other grounds by *California* v. *Acevedo*, 500 U.S. 565 (1991).

Once law enforcement officers have arrested an individual and seized his or her cell phone, there is no possibility that the arrestee himself will be able to act to delete the information it contains. Accordingly, the "preservation of evidence" prong of *Chimel* is also inapplicable.

The government argues (No. 13-212 U.S. Br. 34-40) for a much more expansive interpretation of this aspect of *Chimel*, asserting that the mere possibility that evidence might be destroyed by the actions of a third party or through a device previously installed by the arrestee is sufficient to trigger the exception. It points to the availability of cell phone "wiping" technology that may be activated by a signal sent by a third party or by the arrestee's failure to enter a code at specified time intervals. *Id.* at 37-39.

That argument is flawed on multiple grounds. To begin with, the consequences of expanding *Chimel*'s rationale to encompass the risk that the arrestee may have taken prior action that would result in destruction of evidence or that third parties would act to destroy evidence would dramatically broaden the government's authority. It always is possible that an

arrestee also could have instructed his accomplices to destroy evidence if he did not return to his home by a specified time. Does that mere possibility mean that officers may undertake a warrantless search of every arrestee's home? Does the possibility that a closed container might be booby-trapped to destroy any incriminating materials that it contained mean that police officers may override *Chadwick*'s limitation on the exception?

No decision of this Court endorses such a broad approach. As we have discussed, this Court has made clear that a search is not permissible once the arrestee cannot gain possession of the potential evidence—which will always be the case after the phone has been seized by the officers.[29]

Moreover, there is no support for the government's implicit contention that the use of wiping technologies is widespread and cannot be counteracted, or that the use of passwords—common in a variety of other contexts—somehow justifies expanding the exception. See No. 13-132 Pet. Br. 22-24.

Finally, "a broad reading of [*Chimel*] is also unnecessary to protect law enforcement * * * evidentiary interests." *Gant*, 556 U.S. at 346. As was the case with respect to the overbroad construction of the search-incident-to-arrest exception rejected in *Gant*, "[o]ther established exceptions to the warrant requirement authorize [searches] under additional cir-

---

[29] As we discuss below (at page 28), the government's argument is really a claim for an across-the-board determination that searches of digitally-stored information are always justified by exigent circumstances–something that is not permissible under exigent search principles.

cumstances when safety or evidentiary concerns demand." *Ibid.*

A warrant is not required if "'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment." *Brigham City* v. *Stuart*, 547 U.S. 398, 403 (2006) (quoting *Mincey* v. *Arizona*, 437 U.S. 385, 393-394 (1978)). One such circumstance occurs when an officer is faced with "the imminent destruction of evidence." *McNeely*, 133 S. Ct. at 1559; see, *e.g.*, *Illinois* v. *McArthur*, 531 U.S. 326, 331 (2001) (concluding that a warrantless seizure of a person to prevent him from returning to his trailer to destroy hidden contraband was reasonable "[i]n the circumstances of the case before us" due to exigency); *Cupp* v. *Murphy*, 412 U.S. 291, 296 (1973) (holding that a limited warrantless search of a suspect's fingernails to preserve evidence that the suspect was trying to rub off was justified "[o]n the facts of this case").

"'[T]he fact-specific nature of the reasonableness inquiry,' demands that we evaluate each case of alleged exigency based 'on its own facts and circumstances.'" *McNeely*, 133 S. Ct. at 1559 (internal citations omitted). If officers have specific knowledge that the contents of a particular phone may be lost due to a wiping program or some other technology, and they believe that the contents cannot be preserved while they seek a warrant, they may be able to satisfy the exigent circumstances test.

Importantly, that exigency could justify only the downloading of the digitally-stored information for purposes of preservation, not a search of that information (police patrol cars increasingly are outfitted with the technology to perform such downloads at

the time and place of arrest). A warrant still would be needed to search the information.

Law enforcement officers also do not need a warrant to observe items within their "plain view." "[A] truly cursory inspection—one that involves merely looking at what is already exposed to view, without disturbing it—is not a 'search' for Fourth Amendment purposes, and therefore does not even require reasonable suspicion." *Arizona* v. *Hicks*, 480 U.S. 321, 328 (1987).

If an incoming call, text message, or other information appears on the face of the phone, an officer may view that information without a warrant. That aspect of the officers' actions in *Wurie* was permissible. 13-212 Pet. App. 2a ("[O]ne of Wurie's cell phones * * * was repeatedly receiving calls from a number identified as 'my house' on the external caller ID screen on the front of the phone[and] [t]he officers were able to see the caller ID screen, and the 'my house' label, in plain view.").

But by going on to "open[] the phone" and press a button to "access the phone's call log," review the call log, and "press[] one more button" to search for the suspect's contact information (Pet. App. 3a), the officers moved beyond merely observing information in plain view. The plain view doctrine accordingly cannot justify the federal government's use of the information gained from the officer's manipulation of the phone.[30]

---

[30] Police officers also may conduct "inventory searches"—"[a]t the stationhouse, it is entirely proper for police to remove and list or inventory property found on the person or in the possession of an arrested person who is to be jailed." *Illinois* v. *Lafayette*, 462 U.S. 640, 646 (1983). An officer therefore could ob-

* * * * *

This Court in *Gant* rejected an expansive interpretation of the search-incident-to-arrest exception in part because it "seriously undervalue[d] the privacy interests at stake." 556 U.S. at 344-345. Law enforcement officers would have been able "to search not just the passenger compartment [of the car] but every purse, briefcase, or other container within that space." *Id.* at 345.

Permitting the police to conduct such a search in connection with every single traffic offense arrest would have "create[d] a serious and recurring threat to the privacy of countless individuals. Indeed, the character of the threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." *Ibid.*

---

serve the exterior of an arrestee's cell phone and include it on the list of the arrestee's property.

"[A]n inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence." *Florida* v. *Wells*, 495 U.S. 1, 4 (1990). It therefore cannot justify a search of the data that is electronically stored on the phone. *United States* v. *Davis*, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011) ("[A] lawful inventory search does not authorize an officer to examine the contents of a cell phone."); *United States* v. *Wall*, 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008), *aff'd*, 343 F. App'x 564 (11th Cir. 2009) ("[T]he Government cannot claim that a search of text messages on [defendant's] cell phones was necessary to inventory the property in his possession. Therefore, the search exceeded the scope of an inventory search and entered the territory of general rummaging."); *United States* v. *Flores*, 122 F. Supp. 2d 491, 494 (S.D.N.Y. 2000) ("[N]either a calendar book nor a cellular telephone is a 'container' that has 'contents' that need to be inventoried for safekeeping in the traditional sense of those terms.").

The broad argument advanced by California and the United States in these cases would, if accepted by this Court, enable police officers to "rummage at will" among individuals' most sensitive personal information—the very types of information whose protection was a core purpose of the Fourth Amendment. That argument should be rejected by this Court here, as it was in *Gant*.

C. The Court Should Reject An Exception To The Warrant Requirement Permitting Searches Of Digitally-Stored Information For Evidence Of The Offense Of Arrest.

The federal government urges the Court to recognize a new exception to the Fourth Amendment's warrant requirement that would allow searches of digitally-stored information on cell phones (and presumably any other portable electronic device) whenever an officer has "reason to believe that it contains evidence of the offense of arrest." 13-212 U.S. Br. 45. The Court should reject that argument and reaffirm that a warrant is required to search these large collections of highly personal information.

Although the government relies on *Gant*, that decision actually weighs against the government's argument. The Court there concluded that "*circumstances unique to the vehicle context* justify a search incident to a lawful arrest when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" 556 U.S. at 343 (emphasis added). It did not adopt the general rule urged by the government here, which would not be limited to the vehicle context but rather would apply across-the-board to any place an arrest occurs and to any item found on the individual's person.

That enormous expansion of the government's authority to conduct warrantless searches is contrary to both precedent and the principles underlying the Fourth Amendment.

The government's argument rests largely on *United States* v. *Rabinowitz*, 339 U.S. 56 (1950); see 13-212 U.S. Br. 16 (citing *Rabinowitz*); *id.* at 46 (citing *Thornton* v. *United States*, 541 U.S. 615, 629 (2004) (Scalia, J., concurring) (relying on *Rabinowitz*)).

But *Chimel* expressly rejected that broad interpretation of *Rabinowitz*, stating that "*Rabinowitz* has come to stand for the proposition, *inter alia*, that a warrantless search 'incident to a lawful arrest' may generally extend to the area that is considered to be in the 'possession' or under the 'control' of the person arrested"; that *Rabinowitz* had been thus "limited to its own facts"; and that a broad construction of the decision was inconsistent with other decisions of this Court and not "supported by a reasoned view of the background and purpose of the Fourth Amendment." 395 U.S. at 759-760. Adopting the government's argument would therefore be inconsistent with *Chimel*.

Searches of digitally-stored information are a particularly inappropriate context in which to adopt a new exception to the warrant requirement, because such a search inevitably will allow police officers to rummage through a large volume of extremely personal information. As discussed above, that is the precise sort of search that led to the adoption of the Fourth Amendment's requirement of a warrant.

Moreover, the government never explains why a warrant requirement would be burdensome in this context. Where officers have secured the portable

electronic device, and there are no exigent circumstances, it should be possible to obtain a warrant in short order. *McNeely*, 133 S. Ct. at 1562-63.

A warrant also serves the important purpose of tailoring the scope of the officers' search of digitally-stored information to fit the justification for the search. See *Maryland* v. *Garrison*, 480 U.S. 79, 84 (1987) (explaining that Fourth Amendment requires that a warrant be limited "to the specific areas and things for which there is probable cause to search" in order to avoid "tak[ing] on the character of the wide-ranging exploratory searches the Framers intended to prohibit"). Given the large amount of sensitive personal information contained on these devices, it often will be appropriate to limit the search to the particular type of information to which the officers' probable cause relates.

The government appears to argue that the police officer's determination that there is reason to believe that the device contains evidence of the crime, and the officer's determination of the appropriate scope of the search, are sufficient substitutes for the judgment of a detached magistrate. But the Framers concluded otherwise, based on their experience with abuses of government investigatory authority, and therefore specifically included the warrant requirement in the text of the Fourth Amendment.

Given the particular importance of the warrant requirement in the context of searches of personal papers and other personal information, the absence of any demonstrated burden on law enforcement, and this Court's precedents, the government's argument should be rejected.

D. A Bright-Line Rule Requiring A Warrant For Searches Of Digitally-Stored Information Will Be Much Easier For Officers To Apply Than Other Proposed Standards.

The Court has consistently recognized the benefits of bright-line rules in the Fourth Amendment context. "A single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront." *Dunaway* v. *New York*, 442 U.S. 200, 213-214 (1979). "[I]f police are to have workable rules, the balancing of the competing interests * * * 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'" *Michigan* v. *Summers*, 452 U.S. 692, 705 n.19 (1981) (quoting *Dunaway*, 442 U.S. at 219-220 (White, J., concurring)).

Requiring a warrant for searches of digitally-stored information would provide clear guidance to police officers. Once the officers concluded that they wanted access to information stored on a portable electronic device, and the relevant information was not in plain view, they would know that a warrant is required (absent case-specific exigent circum-

stances).[31] Other proposed standards would create confusion and uncertainty.

1. There Are No Clear Distinctions Between "Smart" And "Dumb" Cell Phones.

No easily ascertainable set of characteristics separate "smart" from "dumb" cell phones—to the contrary the two categories overlap significantly. Thus, the TracFone Prepaid Cell Phone, sold at Walmart for $14.88, includes mobile web access, video recorder, instant messaging, an MP3 player, voice recorder with playback capability, a camera, text messaging capability, a calendar, and a phonebook that can hold 1,000 entries. *TracFone LG440G Cell Phone*, Walmart, http://perma.cc/RDR2-JCLY; see also note 6, *supra*.

Certainly phones are not labeled "smart" or "dumb." Police officers cannot be expected to stay abreast of the latest cell phone developments to distinguish quickly between the myriad of different phone models. And many recent "dumb" phones have the sleek design typically associated with smart phones.[32]

Moreover, cell phones are only one of the many categories of portable electronic devices to which police officers would have to apply this hazy distinc-

---

[31] The burden of obtaining a warrant is no greater in this context than it is in other contexts in which there is no exception to the general standard prescribed by the Fourth Amendment. And advances in technology have made it much easier to obtain a warrant expeditiously. *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1562-1563 (2013).

[32] See, *e.g.*, Stephanie Mlot, *'Premium' Nokia 515 Feature Phone Unveiled*, P.C. Magazine (Aug. 28, 2013, 4:06 PM), http://perma.cc/N3ZJ-C8SQ.

tion. They also would have to be knowledgeable about different models of tablets, laptops, and digital cameras, among other devices.

Finally, any distinction along these lines would quickly become obsolete. As technology advances, production of today's "dumb" devices will cease, today's "smart" devices will become relatively "dumber," and new "smarter" smart devices will enter the marketplace.

Officers on the street simply could not keep themselves aware of the information needed to apply this distinction, assuming that some distinction between types of devices could even be delineated. The result would be rampant confusion.

2. Permitting Law Enforcement Officers To Access Only Certain Types Of Digitally-Stored Information Is Wholly Impractical.

Modern cell phones and other portable electronic devices do not limit a user's access to particular categories of information. To the contrary, the stored information is not compartmentalized and one of the purposes of the phone's applications is to link the various types of information to improve the phone's utility.

For example, "many of the most popular smartphone apps for Apple and Android devices— Twitter, Foursquare and Instagram among them— routinely gather the information in personal address books" for use in those apps.[33] The National Security Agency

---

[33] Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. Times (Feb. 15, 2012, 9:05 AM), http://perma.cc/VZP7-R4TR.

found that certain popular phone apps access sensitive personal information contained on the phone relating to location, age, gender, and sexual orientation.[34] Because data on the phone is so interconnected, a rule permitting police to search some subset of the information simply is not workable.

Moreover, permitting an officer to "look at" only the phone's call log opens the door to fishing expeditions. Police officers will claim that "in the process of" finding the call log they accidentally happened upon other information—a diary, photographs, text messages, emails—and that the other information is admissible on "plain view" grounds. The Court should not adopt a legal standard susceptible to such manipulation, particularly in light of the highly personal nature of the large amounts of information stored on these devices.

An additional flaw in this approach is that a police officer on the street, in the heat of the moment of arrest, often will not be able to determine whether the data he or she is accessing is stored on the electronic device or stored remotely on a server. The federal government acknowledges (No. 13-212 U.S. Br. 34-44) that the search-incident-to-arrest exception cannot justify searches of remotely-stored information. That fact weighs heavily against permitting warrantless searches of particular categories of information.

Apps on cell phones seamlessly integrate local and remotely stored data, making it all but impossi-

---

[34] James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, The Guardian (Jan. 28, 2014, 2:51 AM), http://perma.cc/3LKY-YDWR.

ble to tell where exactly the data displayed on the screen is coming from. In fact, official design principles for both Apple's iOS operating system for iPhones and Google's Android operating system *emphasize* a user experience that obfuscates the difference between local and remote data for the end user. See *iOS Human Interface Guidelines* 62 (2014), http://perma.cc/M5DA-24DR ("[P]eople shouldn't be faced with anything that encourages them to think about file metadata or locations[.]"); *id.* at 101-102 ("Ideally, users don't need to know where their content is located[.] * * * Avoid asking users to choose which documents to store in iCloud."); *Design Principles*, Android Developer, http://perma.cc/N534-576H ("Save what people took time to create and let them access it from anywhere. Remember settings, personal touches, and creations across phones, tablets, and computers.").

Some apps provide a live video feed into a person's home—and more. See, *e.g.*, Somak R. Das et al., *Home Automation and Security for Mobile Devices*. 2011 IEEE International Conference on Pervasive Computing and Communications Workshops 141, 141 (describing the design of a phone-app-based system that "operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video and records it for future playback, and finally manages operations on home appliances, such as turning ON/OFF a television or microwave or altering the intensity of lighting around the house"). Cf. *Kyllo*, 533 U.S. at 35-36 (discussing "imaging technology that could discern all human activity in the home").

An officer could not reliably determine whether, by opening an app, he was looking at a local copy of a

stored email or at emails stored remotely, or whether the personal pictures found were stored on the phone or were instead located on the user's private online photo album (or another individual's online photo album). Law enforcement officers will not be able to make a distinction that is designed by software developers to be essentially invisible.

3. Distinguishing Between Searches At The Place Of Arrest And Searches At The Police Station Would Increase The Intrusion On Privacy Interests Protected By The Fourth Amendment.

The petitioner in No. 13-132 suggests (Pet. Br. 44-53) that the Court could resolve that case by holding that a search conducted remotely from the time and place of arrest violates the Fourth Amendment. Whatever the legal merit of that proposition (compare *United States* v. *Edwards*, 415 U.S. 800 (1974)), a legal standard that permits searches at the time and place of arrest would open the door to warrantless searches of large volumes of highly personal information.

To begin with, such a standard would not impose any practical limitation on these searches. Police cars today typically are outfitted with laptop computers and other devices that can be used to download and search digitally-stored information. Thus, one global survey found that 44% of respondents "now extract mobile data in the field." *Trends shaping mobile forensics in 2014*, http://perma.cc/R8EA-GBP2.

A legal rule that permits police to search all digitally-stored data at the place of arrest without a warrant, but requires a warrant for any subsequent

search, would create a strong incentive *always* to search that information at the scene—and therefore is likely to produce more frequent warrantless searches of this personal information and therefore greater intrusions on the privacy interests protected by the Fourth Amendment.

CONCLUSION

The judgment of the court of appeal in No. 13-132 should be reversed and the judgment of the court of appeals in No. 13-212 should be affirmed.

Respectfully submitted.

EUGENE R. FIDELL
Yale Law School
Supreme Court Clinic
127 Wall St.
New Haven, CT 06511
(203) 432-4992

ANDREW J. PINCUS
Counsel of Record
CHARLES A. ROTHFELD
MICHAEL B. KIMBERLY
PAUL W. HUGHES
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

MARCH 2014

AMICUS CURIAE BRIEF

RECORD AND BRIEFS

Supreme Court U.S.
FILED
MAR 1 3 2014
OFFICE OF THE CLERK

Nos. 13-132 & 13-212

IN THE

Supreme Court of the United States

DAVID LEON RILEY,
Petitioner,

v.

STATE OF CALIFORNIA,
Respondent.

UNITED STATES OF AMERICA,
Petitioner,

v.

BRIMA WURIE,
Respondent.

On Writs of Certiorari to the California Court of Appeal, Fourth District and the U.S. Court of Appeals for the First Circuit

---

Brief of Constitutional Accountability Center as *Amicus Curiae* in Support of Petitioner Riley and Respondent Wurie

---

DOUGLAS T. KENDALL
ELIZABETH B. WYDRA*
**Counsel of Record*
BRIANNE J. GOROD
CONSTITUTIONAL ACCOUNTABILITY CENTER
1200 18th St., NW, Suite 501
Washington, D.C. 20036
(202) 296-6889
elizabeth@theusconstitution.org
Counsel for Amicus Curiae

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTEREST OF *AMICUS CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 1

ARGUMENT 5

I. The Framers Viewed the Fourth Amendment as a Fundamental Protection Against the Use of "General Warrants" 6

II. Permitting Broad Searches of Cell Phones Incident to Arrest Undermines the Fundamental Protections of the Fourth Amendment 16

CONCLUSION 21

TABLE OF AUTHORITIES

Page(s)

Cases

Arizona v. Gant,
556 U.S. 332 (2009) 18

Berger v. State of New York,
388 U.S. 41 (1967) 12

Boyd v. United States,
116 U.S. 616 (1886) 12

Chandler v. Miller,
520 U.S. 305 (1997) 16

Chimel v. California,
395 U.S. 752 (1969) 18

City of Ontario, Cal. v. Quon,
130 S. Ct. 2619 (2010) 20

Marcus v. Search Warrants of Property at 104 East Tenth Street, Kansas City, Mo.,
367 U.S. 717 (1961) 8

Maryland v. King,
133 S. Ct. 1958 (2013) 7, 13, 14, 17, 18

United States v. Chadwick,
433 U.S. 1 (1977) 6

Warden, Md. Penitentiary v. Hayden,
387 U.S. 294 (1967) 16

TABLE OF AUTHORITIES—continued

Page(s)

Wilkes v. Wood,
98 Eng. Rep. 489 (1763) 10

Constitutional Provisions and Legislative Materials

U.S. CONST. amend. IV ..... *passim*

Annals of Congress, 1st Cong. 1st Sess. (1789)..... 15

Virginia Declaration of Rights § 10 13

Books, Articles, and Miscellaneous

Letter from John Adams to William Tudor (March 29, 1817), *in* THE WORKS OF JOHN ADAMS (Boston, Little Brown & Co. 1856) 12

Akhil Reed Amar, *The Bill of Rights as a Constitution,* 100 Yale L.J. 1131 (1991)..... 10

WILLIAM CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING (2009) ... *passim*

Thomas Y. Davies, *Recovering the Original Fourth Amendment,* 98 Mich. L. Rev. 547 (1999)..... 11, 13

Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure,* 103 J. Crim. L. & Criminology 49 (2013)..... 17

DEBATES ON THE FEDERAL CONSTITUTION (J. Elliot 2d ed. 1854)..... 14

TABLE OF AUTHORITIES—continued

Page(s)

Charles E. MacLean, *But, Your Honor, A Cell Phone is not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L. Rev. 37 (2012) 19

Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. Rev. 925 (1997) 9

Letter from James Madison to George Eve (Jan. 2, 1789), *at* http://bit.ly/134r6nw 15

Hon. M. Blane Michael, Madison Lecture, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 905 (2010) ..... *passim*

Brief of Otis, *Paxton's Case* (Mass. Sup. Ct. 24-26 Feb. 1761), Massachusetts Spy, Thu. 29 Apr. 1773 (vol. 3, no. 117) 9

JAMES OTIS, IN OPPOSITION TO WRITS OF ASSISTANCE (1761) 9

Eric Schnapper, *Unreasonable Searches and Seizures*, 71 Va. L. Rev. 869 (1985) 11

Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 Ga. L. Rev. 1165 (2008) 19

TABLE OF AUTHORITIES—continued

Page(s)

JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES (1833).. 6, 7

INTEREST OF AMICUS CURIAE[1]

Amicus Constitutional Accountability Center (CAC) is a think tank, public interest law firm, and action center dedicated to fulfilling the progressive promise of our Constitution's text and history. CAC works in our courts, through our government, and with legal scholars to improve understanding of the Constitution and preserve the rights and freedoms it guarantees. CAC has a strong interest in ensuring that the Constitution applies as robustly as its text and history require and accordingly has an interest in this case.

INTRODUCTION AND SUMMARY OF ARGUMENT

The text and history of the Fourth Amendment establish that police may not engage in generalized searches lacking in individualized suspicion. Indeed, the Framers adopted the Fourth Amendment in large part to guard against the significant intrusions into privacy that could result if the government enjoyed unlimited discretion to search people's homes and belongings. In an age when people keep vast stores of personal information and documents on their cell phones

---

[1] The parties have consented to the filing of this brief and their letters of consent have been filed with the Clerk. Under Rule 37.6 of the Rules of this Court, *amicus* states that no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amicus* or its counsel made a monetary contribution to its preparation or submission.

and other digital devices, the invasion of privacy involved in searches of those devices will often be similar in degree to (if not more substantial than) the intrusion on privacy that results from the search of an individual's home, personal papers, and effects. By permitting the police to search the digital contents of an arrestee's cell phone without first obtaining a warrant, even after the phone has been removed from the arrestee, the California Supreme Court and other courts around the country have given the police unfettered discretion to engage in broad invasions of individual privacy. These decisions should not be allowed to stand.

When the Framers drafted the Fourth Amendment, which broadly provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," and that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," they were responding, in large part, to the British use of "general warrants" and "writs of assistance." These warrants and writs lacked any specificity about the people or items to be searched and were not predicated on any individualized suspicion; essentially unlimited in scope, these warrants and writs allowed the officers executing them virtually unfettered discretion to engage in broad searches of a person's home and the personal papers and effects in that home.

As early as the 1600s, the use of such warrants came under attack in Great Britain. They were decried as an instrument of arbitrary power, and popular opposition to them quickly solidified as they were used to harass critics of the Crown and trample personal liberty. The British nonetheless continued to use general warrants, including in the colonies. During the 1700s, colonial opposition to the use of such warrants grew, and their use was one of the grievances that prompted the call for independence from British rule.

Concerns about the abusive use of general warrants continued in the post-colonial period, and calls for the nation's new Constitution to include an explicit prohibition on the use of general warrants produced what would become the Fourth Amendment. The text of the Fourth Amendment, both as originally drafted and in the form that was ultimately adopted, reflects the Framers' staunch opposition to the use of general warrants. It required not only that all searches be reasonable, but also that all warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. This detailed text enshrines a specific prohibition against general warrants in our nation's charter, and reflects the Framers' more general concern that government officers not be able to search a person's home, papers, and effects in the absence of some individualized, justified suspicion that a specific search would produce evidence of wrongdoing. Stated simply, the Framers wanted to strip the government of the arbitrary power to

rifle through a person's belongings in the hope of finding something incriminating.

The searches in the cases now before the Court both violated this fundamental Fourth Amendment precept. The contents of Petitioner David Riley's cell phone were searched without a warrant and without exigent circumstances, first at the scene of his arrest and then hours later at the police station. Similarly, Respondent Brima Wurie's phone was searched without a warrant and without exigent circumstances. None of the traditional justifications for warrantless searches incident to a lawful arrest can justify the searches of these cell phones—the phones had been removed from the defendants, thus eliminating any concern about destruction of evidence, and it is difficult to see how the text messages, emails, photos, call logs, and other digital contents of the phones could have posed any threat, let alone an imminent threat, to the arresting officers' safety. To the contrary, as the detective who searched Riley's phone hours after the arrest acknowledged, he dug through "'a lot of stuff" on the phone specifically "'looking for evidence.'" Riley J.A. 11, 20. These are precisely the type of searches for which the Constitution demands a warrant.

Allowing law enforcement officers to look through the contents of an arrestee's cell phone without a warrant and in the absence of recognized exigent circumstances invites law enforcement to engage in the same sort of generalized searches that the Framers abhorred—and adopted the Fourth Amendment to prevent. Because modern

cell phones generally contain significant amounts of information, often including sensitive communications and private photographs, the intrusion into an individual's privacy when police rummage through the contents of these phones, particularly smart phones, is substantial. Indeed, because a person may store much of his most private information on his cell phone, the invasion of privacy involved in such searches will often be more substantial than the intrusion on privacy that occurred when individuals' homes—and their personal papers and effects—were searched by overreaching British colonial officers during the Founding era. This Court should hold that, absent exigent circumstances, the warrantless search of an arrestee's cell phone violates the Fourth Amendment.

ARGUMENT

By permitting the police to search the digital contents of an arrestee's cell phone without first obtaining a warrant, even after the phone has been removed from the arrestee, the California Supreme Court and other courts around the country have given the police unfettered discretion to engage in broad invasions of individual privacy. It was just this sort of generalized search, undertaken without probable cause or particularized suspicion, that the Fourth Amendment was adopted to prevent. This Court should hold that the Fourth Amendment's text and history prohibit warrantless searches like the ones that took places in the cases now before the Court.

I. The Framers Viewed the Fourth Amendment as a Fundamental Protection Against the Use of "General Warrants"

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. As the text suggests, the Framers incorporated this fundamental safeguard of liberty into the Constitution to limit the discretion of government officers to engage in general searches unsupported by specific, articulable suspicion, and to prevent the broad invasions of privacy that such searches could entail. This safeguard was "indispensable to the full enjoyment of the rights of personal security, personal liberty, and private property." JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1895 (1833).

The Fourth Amendment's broad protections were in large part a response to specific abuses the Framing generation had suffered under British rule—namely, the use of "general warrants" and "writs of assistance" that lacked specificity as to the person and place to be searched and were not based on any individualized suspicion. *See, e.g.*, *United States v. Chadwick*, 433 U.S. 1, 7-8 (1977) ("It cannot be doubted that the Fourth Amendment's commands grew in large measure out of the

colonists' experience with the writs of assistance and their memories of the general warrants formerly in use in England."); *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting) (noting that the Framers "despised" the use of general warrants); Hon. M. Blane Michael, Madison Lecture, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 905, 906 (2010) (noting that "the British Crown's unbridled power of search . . . is at the center of the rich history that led to the adoption of the Fourth Amendment"); *id.* at 907 ("The Fourth Amendment owes its existence to furious opposition in the American colonies to British search and seizure practices, particularly in the area of customs enforcement."). As Joseph Story observed, the Fourth Amendment's "introduction into the amendments was doubtless occasioned by the strong sensibility excited, both in England and America, upon the subject of general warrants almost upon the eve of the American Revolution." STORY, COMMENTARIES § 1895. Such warrants were despised by Americans as the tools of an arbitrary and unlimited government, used to harass and oppress the people.

General warrants had long been used in Great Britain. For example, the Act of Frauds of 1662 "empowered customs officers in England to enter 'any house, shop, cellar, warehouse or room, or other place' and to 'break open doors, chests, trunks and other package[s]' for the purpose of seizing any 'prohibited and uncustomed' goods."

Michael, 85 N.Y.U. L. Rev. at 907.[2] These warrants were also used to limit the publication of materials critical of the government. *See Marcus v. Search Warrants of Property at 104 East Tenth Street, Kansas City, Mo.*, 367 U.S. 717, 726 (1961) (noting that in the mid-seventeenth century, the Parliament's asserted need for "a broad search and seizure power to control printing" resulted in the issuance of warrants that "often gave the most general discretionary authority"); *see also id.* at 724 ("Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power.").

As early as the mid-1600s, the use of these general warrants came under attack in Great Britain when Edward Coke "became the first of many English legal thinkers to deny the legality of general warrants." WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 105 (2009). "By the end of the century, at least four legal treaties had mentioned Coke's language against general warrants as legal fact," *id.* at 121, and the popularity of Coke's views continued to spread in the ensuing years, as other "legal treatises recited Coke on general warrants as doctrine," *id.*

Despite the growing opposition to the use of general warrants in Great Britain, they remained

---

[2] In 1696, "the broad enforcement powers in the 1662 Act" were extended "to customs officers in the colonies, authorizing the officers to conduct warrantless searches at their discretion." Michael, 85 N.Y.U. L. Rev. at 907.

the standard method of search in the colonies as of the mid-eighteenth century. *See* Tracy Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. Rev. 925, 940 (1997). Colonial opposition to the use of general warrants was galvanized by a series of events on both sides of the Atlantic on the eve of the American Revolution.

In the high-profile Paxton's Case, for example, a group of Boston merchants challenged customs officials' use of general warrants, CUDDIHY, THE FOURTH AMENDMENT, at 380, attacking them as "'the worst instrument of arbitrary power, the most destructive of English liberty . . . that ever was found in an English law-book.'" Michael, 85 N.Y.U. L. Rev. at 908. The merchants' attorney, James Otis, argued that such warrants "place[] the liberty of every man in the hands of every petty officer." JAMES OTIS, IN OPPOSITION TO WRITS OF ASSISTANCE, http://bartleby.com/268/8/9 (last visited July 24, 2013); *see* Michael, 85 N.Y.U. L. Rev. at 908 (noting that Otis called the writ of assistance an "'instrument[] of slavery on the one hand, and villainy on the other'"). According to Otis, writs of assistance could be legal only if they were much more specific, providing for the "search [of] *certain houses* &c. *especially set[ting] forth*, . . . *upon oath made* . . . by the person who asks *that he suspects such goods to be concealed in* THOSE VERY PLACES HE DESIRES TO SEARCH." CUDDIHY, THE FOURTH AMENDMENT, at 377-78 (quoting Brief of Otis, *Paxton's Case* (Mass. Sup. Ct. 24-26 Feb. 1761), *Massachusetts Spy*, Thu., 29 Apr. 1773 (vol. 3, no. 117), p. 3, col. 1). Although the writs in

Paxton's Case were granted, the decision prompted public resistance, and the Massachusetts legislature responded by reducing the judges' salaries and passing a law requiring the use of specific warrants. CUDDIHY, THE FOURTH AMENDMENT, at 403-04; *cf.* Michael, 85 N.Y.U. L. Rev. at 908 (noting that this case "galvanized support for what became the Fourth Amendment").

In the years that followed, colonial opposition to general warrants continued to grow, in part in response to events in Great Britain. When a publication was released that criticized the King, the British Secretary of State issued a general warrant to authorize sweeping searches of forty-nine individuals who might be responsible. John Wilkes, the primary target of the investigation, sued those responsible for executing the warrant. In one of the resulting trials, Chief Justice Pratt of the Court of Common Pleas declared general warrants to be "illegal, and contrary to the fundamental principles of the constitution." *Wilkes v. Wood*, 98 Eng. Rep. 489, 499 (1763). This case was widely covered in American newspapers, and "the reaction of the colonial press to that controversy was intense, prolonged, and overwhelmingly sympathetic to Wilkes." CUDDIHY, THE FOURTH AMENDMENT, at 538; *see id.* at 539 (discussing the scope of the coverage in the colonial press); *id.* at 538 (noting that a "revulsion to general warrants ensued in the colonies" following the Wilkes controversy); *cf.* Akhil Reed Amar, *The Bill of Rights as a Constitution*, 100 Yale L.J. 1131, 1176 (1991) ("Madison's choice of language [in the Fourth

Amendment] may well have been influenced by the celebrated 1763 English case of Wilkes v. Wood, one of the two or three most important search and seizure cases on the books in 1789." (internal footnote omitted)).[3]

Despite the growing opposition to general warrants, Parliament in 1767 again authorized their use in the colonies. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 566 (1999). Some of the local courts in the colonies resisted, refusing to issue the broad, general writs authorized by the Act and instead issuing the more specific warrants lauded by Otis. CUDDIHY, THE FOURTH AMENDMENT, at 519. But "[g]eneral warrants and affiliated methods were still central to colonial search and seizure in 1776." *Id.* at 538.

---

[3] The Wilkes controversy also brought to the fore the public's opposition to the search and seizure of private papers. *See* Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869, 887-94 (1985). The search and seizure of private papers was viewed as a particularly intrusive invasion of privacy because, in part, such papers often "contain[ed] an individual's most private thoughts" and could "expose [the] confidences" of other people. *Id.* at 890. Moreover, "[b]ecause papers cannot so easily be distinguished from each other, a typical search for a document is necessarily a rummaging search of the most intrusive kind." *Id.* at 918. This controversy and the ensuing debates in Britain also influenced thinking in the colonies and helped shape the protections provided by the Fourth Amendment. *See id.* at 920 ("Read in light of its historical background, the fourth amendment's search and seizure clause condemns the inspection of innocent private papers by government officials in search of a document that by itself may be unprotected.").

The colonists' animosity toward general warrants was one of the grievances that caused them to seek independence from Great Britain. As John Adams would later remark, Otis's fiery attack on the practice in *Paxton's Case* "was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." Michael, 85 N.Y.U. L. Rev. at 909 (quoting Letter from John Adams to William Tudor (March 29, 1817) *in* THE WORKS OF JOHN ADAMS 247-48 (Boston, Little Brown & Co. 1856)). Indeed, the colonists attached great importance to the issue of general warrants as they contemplated breaking ties with Great Britain. *See, e.g.*, *id.* at 911 ("the First Continental Congress in 1774 included customs searches under general writs of assistance in its list of grievances against Parliament"); *see also Berger v. State of N.Y.*, 388 U.S. 41, 58 (1967) (noting that the use of general warrants "was a motivating factor behind the Declaration of Independence"); *Boyd v. United States*, 116 U.S. 616, 625 (1886) (describing the debate in which Otis's speech occurred as "perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country").

After the War for Independence was won, the colonists' fight to end the use of general warrants continued. Their use initially remained common in the new nation, CUDDIHY, THE FOURTH AMENDMENT, at 602 ("General warrants proliferated and remained the keystone of American laws and practices regarding search and

seizure until at least 1782."). But the "specific warrant ultimately won out." *Id.* By 1784, Vermont and half of the original thirteen states had "formulated constitutions with restrictions on search and seizure," although the precise formulations of those restrictions varied. *Id.* at 603; *see King*, 133 S. Ct. at 1980-81 (Scalia, J., dissenting) (quoting, for example, the Virginia Declaration of Rights § 10, which provided that "general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed," or to search a person "whose offence is not particularly described and supported by evidence," "are grievous and oppressive, and ought not be granted").[4]

When the Framers gathered to draft the new federal Constitution, concerns about potential abuses of governmental authority through the use of general warrants were raised. *See* Davies, 98 Mich. L. Rev. at 583. Indeed, the Constitution's failure to provide any protection against general warrants was a favorite topic of Anti-Federalist writers, at least 15 of whom penned objections to the Constitution on that ground. CUDDIHY, THE FOURTH AMENDMENT, at 674; *see id.* ("The general warrant attracted the earliest and heaviest criticism."); *King*, 133 S. Ct. at 1981 (Scalia, J.,

---

[4] The introduction of constitutional prohibitions on the use of general warrants did not result in the complete elimination of such searches in the States, CUDDIHY, THE FOURTH AMENDMENT, at 624, 628, but these constitutional provisions were nonetheless the "direct ancestors" of the Fourth Amendment, *id.* at 603.

dissenting) ("Antifederalists sarcastically predicted that the general, suspicionless warrant would be among the Constitution's 'blessings'"). Patrick Henry, for example, "warned that the new Federal Constitution would expose the citizenry to searches and seizures 'in the most arbitrary manner, without any evidence or reason.'" *King*, 133 S. Ct. at 1981 (Scalia, J., dissenting) (quoting 3 DEBATES ON THE FEDERAL CONSTITUTION 588 (J. Elliot 2d ed. 1854)). Another critic of the new Constitution described "the absence of security against [general] warrants as part of an 'extraordinary' failure by Congress to safeguard the people's rights." CUDDIHY, THE FOURTH AMENDMENT, at 674. James Otis's sister, Mercy Otis Warren, joined the fight, "assail[ing] writs of assistance" as "'a detestable instrument of arbitrary power.'" *Id.* at 677.

Several state ratifying conventions requested more explicit protection. The Fourteenth Amendment of Virginia's proposed Bill of Rights reflected Anti-Federalists' concerns about general warrants, providing, in pertinent part, that "all general warrants to search suspected places, or to apprehend any suspected person, without specially naming or describing the place or person, are dangerous and ought not to be granted." *Id.* at 684. New York, North Carolina, and Rhode Island copied Virginia's search and seizure amendment with minimal alteration. *Id.* at 685. The arguments presented in favor of including an express prohibition on general warrants in the federal constitution received consistent and nationwide newspaper coverage, and "[t]he magnitude of that publicity indicated the

emergence of a consensus for a comprehensive right against unreasonable search and seizure." *Id.* at 686.

Although the Federalists initially believed that there was no need to add a Bill of Rights to the Constitution, by 1789, James Madison had decided the Constitution should be amended to expressly protect a number of "essential rights" not explicitly protected in the new Constitution, including the "security against general warrants." Letter from James Madison to George Eve (Jan. 2, 1789), *at* http://bit.ly/134r6nw. The initial text of Madison's proposed amendment made clear the importance that he attached to individualized and particularized suspicion as predicates for governmental searches: "The rights of the people to be secured in their persons, their houses, their papers, and their other property from all unreasonable searches and seizures, shall not be voided by warrants . . . not particularly descrybing the places to be searched, or the persons or things to be seized." 1 *Annals of Cong.* 452 (1789) (Joseph Gales ed., 1790). The language was subsequently modified in committee, but the requirement of specific warrants remained materially unchanged. CUDDIHY, THE FOURTH AMENDMENT, at 695-97.

The Fourth Amendment thus enshrines in our national charter the Framers' opposition to generalized searches that were not predicated on any individualized suspicion. As the next section demonstrates, warrantless cell phone searches like the ones that took places in the cases now before the Court violate that core Fourth Amendment

principle, even though those searches were incident to lawful arrests.

II. Permitting Broad Searches of Cell Phones Incident to Arrest Undermines the Fundamental Protections of the Fourth Amendment

As explained above, the Fourth Amendment was a response, in significant part, to the abusive use of general warrants by the British, but its adoption also reflected a broader concern about the intrusions into privacy that could result if the government enjoyed unlimited discretion to search people's homes and belongings. Michael, 85 N.Y.U. L. Rev. at 906 (noting the "broader purpose of the Amendment: to circumscribe government discretion"); CUDDIHY, THE FOURTH AMENDMENT, at 679 (noting an Anti-Federalist "desire to divest the central government not only of [the general warrant] but of all relatives of it that jeopardized privacy"). Thus, as this Court has repeatedly recognized, a core concern of the Fourth Amendment is ensuring that the government has individualized suspicion about wrongdoing before it intrudes on a person's privacy. *See, e.g.*, *Chandler v. Miller*, 520 U.S. 305, 308 (1997) (explaining that the Fourth Amendment's "restraint on government conduct generally bars officials from undertaking a search or seizure absent individualized suspicion"); *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (explaining that the Fourth Amendment was "a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies, and was intended to protect against

invasions of 'the sanctity of a man's home and the privacies of life' from searches under indiscriminate, general authority" (internal citation omitted)); *King*, 133 S. Ct. at 1982 (Scalia, J., dissenting) ("suspicionless searches are *never* allowed if their principal end is ordinary crime-solving").

Allowing the police to search the contents of an individual's cell phone without a warrant violates this fundamental Fourth Amendment precept because it permits exactly the sort of generalized search lacking in particularized suspicion (and the concomitant invasion of privacy) that the Fourth Amendment's requirement for particularized warrants was supposed to prevent. That such searches are triggered by an arrest does little to limit the government's discretion because arrests are often triggered by minor legal infractions; as Petitioner Riley notes, "in California as in most other states, the police may—and sometimes do—arrest people for traffic and other 'fine only' infractions such as jaywalking, littering, or riding a bicycle the wrong direction on a residential street." Riley Pet. Br. 2; *see* Wurie Pet. App. 19a (noting that the Government's proposed rule would allow cell phone searches "even for something as minor as a traffic violation").[5]

---

[5] To the extent such searches disclose an individual's papers (as they often will), they are especially problematic in light of the Fourth Amendment's special protections for personal papers. *See supra* at 11 n.3; *see also* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 101, 109 (2013) (discussing

Moreover, that the individual whose phone is being searched was arrested is not sufficient to justify such a broad invasion of privacy. As this Court recently noted, the fact that a person is in custody following arrest cannot justify all searches, regardless of the level of privacy invaded, *King*, 133 S. Ct. at 1979, and the traditional justifications for searches incident to arrest have no bearing once the cell phone has been removed from the arrestee's control, *see* Riley Pet. Br. 16-24; *see also Chimel v. California*, 395 U.S. 752, 763 (1969) (setting out the twin purposes of searches incident to arrest, *viz.*, "remov[ing] any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape" and "seiz[ing] any evidence on the arrestee's person in order to prevent its concealment or destruction"); *Arizona v. Gant*, 556 U.S. 332, 339 (2009) ("If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply."). Further, because of the vast stores of information that are generally saved on modern cell phones, the invasion of privacy inherent in such a search is significantly greater than the invasion involved in

---

Learned Hand's "anti-rummaging" principle which held that "the police had no more constitutional power upon arrest than a judge issuing a warrant to comb through a vast trove of innocent papers in quest of an illegal one" and arguing that "[t]he anti-rummaging principle . . . suggests curtailing the warrantless seizure and search of digital devices incident to arrest").

previous search-incident-to-arrest cases, involving, for example, physical containers with much more limited and physical contents. *See* Riley Pet. Br. 3 ("Americans use smart phones to generate and store a vast array of their more sensitive thoughts, communications and expressive material."); *id.* at 14 ("[l]aw developed with only physical objects in mind cannot be woodenly applied to digital files containing virtually limitless amounts of information").

Modern cell phones are unique, after all, in that they permit individuals to carry significant amounts of personal information and documents that would previously have been kept in the home and office. Indeed, they are like computers in their ability to store vast amounts of information. *See, e.g.*, Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 Ga. L. Rev. 1165, 1172 (2008) (noting that cell phones have been described as "microcomputers"); *id.* at 1201 ("The more advanced devices are practically hand-held computers with telephone capabilities, giving the user access to a wealth of public and private data stored online and in the device's memory.").[6] Thus, they will often contain not only phone call records and a rolodex of the owner's

---

[6] The storage capacities of modern cell phones are staggering. For example, "modern cell phones are capable of storing at least sixty-four gigabytes of private information equaling four million pages of Microsoft Word documents." Charles E. MacLean, *But, Your Honor, A Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L. Rev. 37, 42 (2012).

contacts (both professional and personal), but also thousands of email messages and texts, photographs, even personal notes. Petitioner Riley's smartphone was "capable of accessing the internet, capturing and storing photos and videos, providing and storing GPS location information, and capturing and storing both voice and text messages, among other features," Riley Pet. Br. 5, and the police search exposed private text messages, the phone's contacts list, photographs, and videos, *id.* at 5-6. Even Respondent Wurie's "comparatively unsophisticated flip phone" (Wurie BIO 12) contained, among other things, call logs and a rolodex of phone numbers. Wurie Pet. App. 3a.

In other words, many documents and effects that would once have been stored physically in a person's home are often now stored in digital form, and a search of a person's cell phone thus invites an invasion of personal privacy that is little different from the invasion of privacy produced by searches of people's homes and papers at the Founding. *See id.* at 18a-19a ("Just as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government's proposed rule would give law enforcement automatic access to 'a virtual warehouse' of an individual's 'most intimate communications and photographs without probable cause' if the individual is subject to a custodial arrest . . . ."); *cf. City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that

some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

The Framers adopted the Fourth Amendment to ensure that the people would be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. This Court should hold that, absent exigent circumstances, the text and history of the Fourth Amendment do not permit police officers to conduct a warrantless search of the digital contents of an individual's cell phone seized from the person at the time of arrest.

CONCLUSION

For the foregoing reasons, *amicus* urges the Court to hold that, absent exigent circumstances, warrantless searches of the digital contents of cell phones incident to arrest violate the Fourth Amendment.

Respectfully submitted,

DOUGLAS T. KENDALL
ELIZABETH B. WYDRA*
*Counsel of Record
BRIANNE J. GOROD
CONSTITUTIONAL
ACCOUNTABILITY CENTER
1200 18th Street NW, Suite 501
Washington, D.C. 20036
(202) 296-6889
elizabeth@theusconstitution.org
Counsel for Amicus Curiae

March 2014

AMICUS CURIAE BRIEF

RECORD AND BRIEFS

Nos. 13-132 & 13-212

Supreme Court, U.S.
FILED
MAR 7 2014
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

DAVID LEON RILEY,
Petitioner,

v.

STATE OF CALIFORNIA,
Respondent.

UNITED STATES OF AMERICA,
Petitioner,

v.

BRIMA WURIE,
Respondent.

On Writs of Certiorari to the California Court of Appeal, Fourth District and the United States Court of Appeals for the First Circuit

BRIEF OF AMICI CURIAE CRIMINAL LAW PROFESSORS IN SUPPORT OF PETITIONER RILEY AND RESPONDENT WURIE

Adam M. Gershowitz
Professor of Law
WILLIAM & MARY
LAW SCHOOL

Patricia E. Roberts
WILLIAM & MARY LAW
SCHOOL APPELLATE AND
SUPREME COURT CLINIC
P.O. Box 8795
Williamsburg, VA 23187
Telephone: 757-221-3821

Tillman J. Breckenridge
(*Counsel of record*)
Tara A. Brennan
REED SMITH LLP
1301 K Street NW
Washington, DC 20005
Telephone: 202-414-9200
Facsimile: 202-414-9299
tbreckenridge@reedsmith.com

Counsel for Amici Curiae Criminal Law Professors

Library of Congress
Law Library

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF AUTHORITIES ii

INTEREST OF AMICI CURIAE 1

SUMMARY OF ARGUMENT 2

ARGUMENT 3

I. Faraday bags Prevent Remote Cell Phone Data wiping, Are Inexpensive, and Are Already widely Used By Law Enforcement. 3

II. Forbidding Warrantless Searches While Allowing Seizures Protects The Balance Of Interests Between The Government And Citizens 8

A. Use of Faraday Envelopes or Aluminum Foil to Preserve Cell Phone Data Would Impose No Burden on Law Enforcement. 8

B. The Court Should Not Apply Arizona v. Gant's "Reasonable To Believe" Standard To Cell Phones. 17

CONCLUSION 25

APPENDIX LISTING AMICI CRIMINAL LAW PROFESSORS 1a

TABLE OF AUTHORITIES

Page(s)

Cases

Arizona v. *Gant*, 556 U.S. 332 (2009) ..... passim

Arkansas v. *Sanders*, 442 U.S. 753 (1979) ... 14, 15, 16

Atwater v. *City of Lago Vista*, 532 U.S. 318 (2001) 20

California v. *Acevedo*, 500 U.S. 565 (1991) 15, 16

California v. *Diaz*, 244 P.3d 501 (Cal. 2011) 11

Chimel v. *California*, 395 U.S. 752 (1969) 3, 8

Connecticut v. *Boyd*, 992 A.2d 1071 (Conn. 2010) 11

Gracie v. *Alabama*, 92 So.3d 806 (Ala. Crim. App. 2011) 11

Illinois v. *MacArthur*, 531 U.S. 326 (2001) 12, 13

New York v. *Belton*, 453 U.S. 454 (1981) 17

Ohio v. *Smith*, 920 N.E.2d 949 (Ohio 2009) 11

Oregon v. *Nix*, 237 P.3d 842 (Or. Ct. App. 2009) 11

Segura v. *U.S.*, 468 U.S. 796 (1984) 13, 25

U.S. v. *Brookes*, No. CRIM2004-0154, 2005 WL 1940124 (D. V.I. June 16, 2005) 9

U.S. v. *Parada*, 289 F. Supp.2d 1291 (D. Kan. 2003) 9

U.S. v. *Aguirre*, 664 F.3d 606 (5th Cir. 2011) 21

U.S. v. *Chadwick*, 433 U.S. 1 (1977) 14

U.S. v. *Cote*, No. 03CR271, 2005 WL 1323343 (N.D. Ill. May 26, 2005) 9

U.S. v. *Dimarco*, No. 12CR205, 2013 WL 444764 (S.D.N.Y. Feb. 5, 2013) 11

U.S. v. *Dixon*, No. 1-12-CR-205, 2013 WL 4718934 (N.D. Ga. Sept. 3, 2013) 11

U.S. v. *Finley*, 477 F.3d 250 (5th Cir. 2007) 9, 21

U.S. v. *Flores-Lopez*, 670 F.3d 803 (7th Cir. 2012) 4, 11

U.S. v. *Gholston*, No. 13-20187, 2014 WL 279609 (E.D. Mich. Jan. 27, 2014) 11

U.S. v. *James*, No. 1:06CR134, 2008 WL 1925032 (E.D. Mo. Apr. 29, 2008) 11

U.S. v. *LaSalle*, No. 07-00032, 2007 WL 1390820 (D. Haw. May 9, 2007) 9

U.S. v. *Mayo*, No. 2:13-CR-48, 2013 WL 5945802 (D. Vt. Nov. 6, 2013) 4

U.S. v. *McGhee*, No. 8:09CR31, 2009 WL 2424104 (D. Neb. July 21, 2009) 18

U.S. v. *Murphy*, 552 F.3d 405 (4th Cir. 2009) 11

U.S. v. *Nyuon*, No. CR.12-40017-01, 2013 WL 943635 (D.S.D. Mar. 11, 2013) 11

U.S. v. *Park*, No. CR05-375, 2007 WL 1521573 (N.D. Cal. May 23, 2007) 11

U.S. v. *Place*, 462 U.S. 696 (1983) 13, 14

U.S. v. *Robinson*, 414 U.S. 218 (1973) 3

U.S. v. *Rocha*, No. 06-40057-01, 2008 WL 4498950 (D. Kan. Oct. 2, 2008) 11

U.S. v. *Ross*, 456 U.S. 798 (1981) 15

U.S. v. *Saldago*, No. 1:09-CR-454, 2010 WL 3062440 (N.D. Ga. June 12, 2010) 9

U.S. v. *Smith*, 715 F.3d 1110 (8th Cir. 2013) 4

U.S. v. *Stephens*, No. 13-200004, 2013 WL 5409907 (W.D. Tenn. Sept. 25, 2013) 9

U.S. v. *Thornton*, 541 U.S. 615 (2004) 17

U.S. v. *Wall*, No. 08-60016, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008) 11, 21

U.S. v. Wurie, 728 F.3d 1 (1st Cir. 2013) 10, 11

Warden v. *Hayden*, 387 U.S. 294 (1967) 8

Wisconsin v. *Carroll*, 778 N.W.2d 1 (Wis. 2010) 9, 10

Statutes

MASS. GEN. LAWS ANN. ch. 90, § 13B 21

N.C. GEN. STAT. ANN. § 20-137.4A 20

N.C. GEN. STAT. ANN. § 29-137.4A 21

N.J. STAT. ANN. § 39:4-97.3 21

R.I. GEN. LAWS § 31-22-30 21

TENN. CODE ANN. § 55-8-199 21

W. VA. CODE ST. R. § 149-7-6.4.6.3.F.1(a) 6

WYO. STAT. ANN. § 346.89 21

Other Authorities

Lt. John Bennett, *Don't Forget the Cell Phone*, CYBER FORENSICS DIV. NEWSLETTER (Armstrong Atl. State Univ. Police, Savannah, Ga.), July/Aug. 2013, http://www.armstrong.edu/images/police/cfdnewsletter.pdf 5

BUREAU OF FORENSIC SERVS., CAL. DEP'T OF JUSTICE, PHYSICAL EVIDENCE BULLETIN: DIGITAL EVIDENCE COLLECTION – MOBILE DEVICES (Dec. 2011), http://oag.ca.gov/sites/all/files/pdfs/cci/reference/peb_18.pdf 6

Karl Dunnagan & Amber Schroader, *Dialing for Evidence*, 2 LAW OFFICER MAGAZINE 46 (Jan./Feb. 2006) 4

Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY BILL RTS. J. 601 (2013) 1, 7, 16

Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 ARIZ. L. REV. 577 (2012) 1, 20

Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27 (2008) 1, 3, 24

Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403 (2013) 18

Graham Kuzia, *Handling Cell Phones and Their Digital Evidence*, POLICE (Apr. 18, 2013), http://www.policemag.com/blog/technology/story/2013/04/cell-phone-seizures.aspx 5

Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403 (2010) 15

Janet Koven Levit, *Pretextual Traffic Stops:* United States *v.* Whren *and the Death of* Terry *v.* Ohio, 28 LOY. U. CHI. L.J. 145 nn.63-64 (1996) 20

Charles E. MacLean, *But, Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 41 (2012) 7

Legal Update Sept. 2013, WEEKLY RAP UP (Monroe Cnty. Sherrif's Office, Stock Island, Fla.), Sept. 2013, https://www.keysso.net/employees/weekly_rap_up/2013/09132013.pdf 5

N.Y. STATE DIV. OF CRIMINAL JUSTICE SERV., ADULT ARRESTS: 2003-2012, http://www.criminaljustice.ny.gov/crimnet/ojsa/arrests/Allcounties.pdf 22

NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS (2d ed. 2008), https://www.ncjrs.gov/pdffiles1/nij/219941.pdf 5

Chenda Ngak, *LulzSec Takes on Arizona Law Enforcement*, CBS NEWS (Aug. 29, 2011, 3:18 PM), http://www.cbsnews.com/news/lulzsec-takes-on-arizona-law-enforcement/ 5

Laurie Segall, *5 Pay-By-Phone Apps Tested*, CNNMONEY (Sept. 24, 2012, 9:31 AM), http://money.cnn.com/gallery/technology/2012/09/24/mobile-payment-apps/index.html 19

Noah Shactman, *Fighting Crime with Cellphones' Clues*, N.Y. TIMES, May 3, 2006, http://www.nytimes.com/2006/05/03/technology/techspecial3/03cops.html?_r=0 4

MG Siegler, *Check-in on Foursquare Without Taking Your Phone Out of Your Pocket*, TECHCRUNCH, Aug. 2, 2010, http://techcrunch.com/2010/08/02/future-checkin/ 23

Dwight Silverman, *Your iPhone Knows Where You've Been, Puts It on a Map*, SEATTLE POST-INTELLIGENCER, Oct. 31, 2013, http://blog.chron.com/techblog/2013/10/your-iphone-knows-where-youve-been-puts-it-on-a-map/ 23

CRIMINAL JUSTICE INFO. SERVS. DIV., U.S. DEP'T OF JUSTICE, TABLE 29: ESTIMATED NUMBER OF ARRESTS (2009), http://www2.fbi.gov/ucr/cius2009/data/table_29.html 19

VA. DEP'T OF FORENSIC SCIS., EVIDENCE HANDLING & LAB. CAPABILITIES GUIDE (Sept. 2012), http://www.dfs.virginia.gov/wp-content/uploads/2013/07/EvidenceGuide.pdf 6

INTEREST OF *AMICI CURIAE*

Amici are criminal procedure professors who teach, study, and write about the Fourth Amendment.[1] *Amici* believe this case presents fundamental issues about how the Fourth Amendment will be interpreted in thousands of cases for decades to come. *Amici* are of the view that search incident to arrest precedent created in a non-digital world cannot be logically applied to cell phones and other mobile electronic devices.

The lead amicus, Adam M. Gershowitz, is a Professor of Law at William & Mary Law School. He has written numerous law review articles analyzing courts' approaches to searching cell phones incident to arrest, including: *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27 (2008); *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125 (2011); *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 ARIZ. L. REV. 577 (2012); *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY BILL RTS. J. 601 (2013).

A list of the other *Amici* who reviewed and join in this brief is included in the attached Appendix.

---

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the *amici curiae* or their counsel made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief.

SUMMARY OF ARGUMENT

The Court should not apply search incident to arrest precedent created in a world of typewriters and carbon paper to digital devices capable of storing a warehouse full of documents, pictures, and GPS location data. Cell phones carry a lesser risk of destruction of evidence and a greater risk of government intrusion on privacy than the limited technologies on which the search incident to arrest doctrine is based. Rather than allowing warrantless searches of cell phones incident to arrest, the Court should encourage law enforcement officers to place cell phones in Faraday envelopes or aluminum foil to prevent the remote wiping of data from the phone while officers seek a warrant.

A Faraday envelope is simply an aluminum-lined container that isolates its contents from outside signals. Law enforcement agencies can purchase Faraday envelopes for only a few dollars. In the alternative, at a cost of only pennies, police can prevent remote wiping by simply wrapping cell phones in a sheet of aluminum foil purchased from a grocery store. Because police departments would only have to equip a small fraction of officers with Faraday envelopes or aluminum foil, the cost would be minimal.

Forbidding warrantless cell phone *searches*, while allowing cell phone *seizures*, incident to arrest is preferable to applying the *Arizona* v. *Gant*, 556 U.S. 332 (2009) "reasonable to believe" formulation to cell phones. Because of the enormous amount of data held on cell phones, it would be reasonable for police to believe evidence of numerous minor crimes might be held on a cell phone. The *Gant* formulation

would therefore fail to offer meaningful privacy protection.

ARGUMENT

I. FARADAY BAGS PREVENT REMOTE CELL PHONE DATA WIPING, ARE INEXPENSIVE, AND ARE ALREADY WIDELY USED BY LAW ENFORCEMENT.

The Court should not apply search incident to arrest precedent created in a world of typewriters and carbon paper to digital devices capable of storing a warehouse full of documents, pictures, and GPS location data. The search incident to arrest doctrine enunciated in *Chimel* v. *California*, 395 U.S. 752 (1969) and *U.S.* v. *Robinson*, 414 U.S. 218 (1973) would fail to afford sufficient privacy protection to private data and would encourage police to unnecessarily rummage through, *inter alia*, reams of text messages, emails, internet browsing history, photographs, and GPS location datalocation information, and myriad other forms of data stored in cell phones. *See* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 44 (2008).

The government interest in preventing destruction of evidence is inapplicable to cell phones because there is a simple solution that can protect private cell phone data while eliminating the risk of remote destruction of evidence: The Court should adopt a rule in which police officers who conduct a lawful arrest are permitted to seize cell phones without a warrant, and then protect evidence on the phones by placing them in a Faraday envelope or wrapping them in aluminum foil while applying for a search warrant.

Despite its unusual name, a Faraday envelope is a very simple and very common item. A "'Faraday bag' or 'Faraday cage' [is] essentially an aluminum-foil wrap or some equivalent, which isolates the cell phone from the phone network and from Bluetooth and wireless Internet signals." *U.S.* v. *Flores-Lopez*, 670 F.3d 803, 809 (7th Cir. 2012) (internal marks omitted). Faraday cages are omnipresent in American households. They are used in microwave ovens to keep the microwaves inside the oven and in coaxial cables to keep radiowaves from interfering with cable transmission. *See id.* (citation omitted). In laymen's terms, once a cell phone is placed inside of a Faraday bag or envelope, the phone can no longer communicate with the outside world and thus cannot be remotely wiped by a conspirator.

Numerous law enforcement agencies already use Faraday bags.[2] The United States Department of

---

[2] *See U.S.* v. *Smith*, 715 F.3d 1110, 1114 (8th Cir. 2013) ("Special Agent Jackson [of the FBI office in St. Louis] then placed the four cell phones and the laptop in a 'Faraday' bag to prevent remote access so the phone could not be remotely wiped."); *U.S.* v. *Mayo*, No. 2:13-CR-48, 2013 WL 5945802, at *11 & n.9 (D. Vt. Nov. 6, 2013) (noting the practice of Vermont State Police to place cell phones in Faraday enclosures); Karl Dunnagan & Amber Schroader, *Dialing for Evidence*, 2 LAW OFFICER MAGAZINE 46, 49 (Jan./Feb. 2006), *available at* http://www.lawofficer.com/article/technology-and-communications/ dialing-evidence (explaining, in an article by a Los Angeles County Sheriff's deputy, that "[t]o remove a handset from the network, use a Faraday bag, such as Pareben's Wireless StrongHold bag"); Noah Shactman, *Fighting Crime with Cellphones' Clues*, N.Y. TIMES, May 3, 2006, http://www.nytimes.com/2006/05/03/technology/techspecial3/03cops.html?_r=0 (noting that "when Detective Reiber [of the Boise, Idaho Police Department] arrives on the scene, he places the phone in a 'Faraday bag,' a container made of triwoven

Justice and other law enforcement agencies have made Faraday bag use part of their policies and procedures.[3] And local law enforcement agencies have encouraged their use.[4] In addition to police

---

copper, nickel, and silver that keeps the phone from making or receiving calls").

[3] *See* NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS 14 (2d ed. 2008), https://www.ncjrs.gov/pdffiles1/nij/219941.pdf ("First responders should also have radio frequency-shielding material such as faraday isolation bags or aluminum foil to wrap cell phones . . . . [to] prevent[] the phones from receiving a call, text message, or other communications signal that may alter the evidence."); *Legal Update Sept. 2013*, WEEKLY RAP UP (Monroe Cnty. Sherrif's Office, Stock Island, Fla.), Sept. 2013, at 1, https://www.keysso.net/employees/weekly_rap_up/2013/09132013.pdf ("When you seize a phone . . . you can ensure that "it cannot send or receive data . . . [by using] a 'faraday' bag."); Chenda Ngak, *LulzSec Takes on Arizona Law Enforcement*, CBS NEWS (Aug. 29, 2011, 3:18 PM), http://www.cbsnews.com/news/lulzsec-takes-on-arizona-law-enforcement/ (discussing internal Arizona memo instructing that "[l]aw enforcement seizing iPhones as potential evidence are recommended to protect the phone from wireless signals . . . through the use of a faraday bag").

[4] *E.g.*, Lt. John Bennett, *Don't Forget the Cell Phone*, CYBER FORENSICS DIV. NEWSLETTER (Armstrong Atl. State Univ. Police, Savannah, Ga.), July/Aug. 2013, at 3, http://www.armstrong.edu/images/police/cfdnewsletter.pdf ("You can disconnect the phone from the network by placing the phone in a Faraday device . . . . The phone can [also] be placed in a copper mesh bag, wrapped in aluminum foil (3-5 times), or simply sealed in a paint can. Keep a roll of aluminum foil in your vehicle for quick and easy access once the device is in possession."); Graham Kuzia, *Handling Cell Phones and Their Digital Evidence*, POLICE (Apr. 18, 2013), http://www.policemag.com/blog/technology/story/2013/04/cell-phone-seizures.aspx (noting in article by North Carolina police

officers and departments that have specifically acknowledged using Faraday bags, other agencies have recommended that approach.[5] Indeed, at least one state has promulgated a regulation encouraging the use of Faraday bags by law enforcement. W. VA. CODE ST. R. § 149-7-6.4.6.3.F.1(a) (instructing law enforcement officers that "[w]ireless mobile devices should be removed from the wireless networks . . . [by] removing the battery or placing the cellular telephone in a Faraday bag/container or wrap[ping] the device in three layers of aluminum foil . . . .").

Faraday bags come in a variety of forms ranging from moderately priced to very inexpensive. On the higher end, and selling for $58, are bags that are equipped with a clear window so that law enforcement can manipulate and examine the phone while protecting it from remote wiping.[6]

---

officer that police should place cell phones in a "Faraday bag, aluminum foil, or signal-blocking container . . . . [to] prevent a third party from connecting to the phone and being able to alter what's on it").

[5] *See, e.g.*, VA. DEP'T OF FORENSIC SCIS., EVIDENCE HANDLING & LAB. CAPABILITIES GUIDE III-6 (Sept. 2012), http://www.dfs.virginia.gov/wp-content/uploads/2013/07/EvidenceGuide.pdf (recommending that cell phones be placed into a "shielded bag" such as the Faraday bag manufactured by Paraben Corporation); BUREAU OF FORENSIC SERVS., CAL. DEP'T OF JUSTICE, PHYSICAL EVIDENCE BULLETIN: DIGITAL EVIDENCE COLLECTION—MOBILE DEVICES 3 (Dec. 2011), http://oag.ca.gov/sites/all/files/pdfs/cci/reference/peb_18.pdf (recommending that mobile phones be placed "in a Faraday bag or similar material (e.g. arson cans, aluminum foil wraps, etc.)").

[6] *See, e.g.*, *Black Hole Faraday Bag—RF Signal Isolation for Forensics, Standard Window Size*, AMAZON, http://www.amazon.com/Black-Hole-Faraday-Bag-isolation/dp/

Police can purchase much cheaper Faraday envelopes—metallic-lined envelopes that have pre-printed chain-of-custody labels on the outside—for only $6.95 each, or at a lower price if purchased in bulk.[7] Even these simpler and cheaper Faraday envelopes can "dramatically reduce or completely eliminate any risk of remotely disturbing a cell phone's internal memory." Charles E. MacLean, *But, Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 41, 54 (2012).

If police departments lack the funding for even the $6.95 Faraday envelope, they can have officers create their own Faraday envelopes for mere pennies by using aluminum foil sold in grocery stores. The essential ingredient in any Faraday device is the aluminum that blocks any signal from reaching the phone. Police need only a small amount of aluminum foil—a tiny fraction of an ordinary roll—to wrap the phone, immobilize it, and prevent the destruction of evidence. *See* Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search*

B0091WILY0/ (last visited Mar. 4, 2014) (noting that the bag was "designed for law enforcement digital forensics").

[7] *See Paraben's Single-Use Stronghold Bags*, PARABEN, CORP., http://www.paraben.com/single-use-stronghold.html (last visited Mar. 4, 2014). The Faraday envelopes are manufactured by a company specializing in computer forensic software. *See About Paraben*, PARABEN, CORP., http://www.paraben.com/about.html (last visited Mar. 4, 2014).

Problem, 22 WM. & MARY BILL RTS. J. 601, 609 (2013). Given that Walmart sells 150 square feet of brand-name aluminum foil for less than $6, and given that about a foot of aluminum foil is sufficient to wrap a cell phone multiple times, the cost for police to create a Faraday enclosure using aluminum foil is about four cents.

Faraday bags, Faraday envelopes, or simple aluminum foil render the only rationale for the search incident to arrest doctrine that could possibly apply to cell phones inapplicable by preventing the destruction of evidence.[8] *See Chimel*, 395 U.S. at 763. Because Faraday devices or aluminum foil work effectively and cheaply, this Court should adopt a rule allowing only a seizure of the cell phone incident to arrest while the police apply for a search warrant.

II. FORBIDDING WARRANTLESS SEARCHES WHILE ALLOWING SEIZURES PROTECTS THE BALANCE OF INTERESTS BETWEEN THE GOVERNMENT AND CITIZENS.

A. Use of Faraday Envelopes or Aluminum Foil to Preserve Cell Phone Data Would Impose No Burden on Law Enforcement.

1. There is no practical limitation on law enforcement officers' ability to carry Faraday bags or foil to wrap cell phones, and the Court's precedents

---

[8] The other rationale for the search incident to arrest doctrine—protecting officer safety—is not plausibly implicated in most cell phone searches. Moreover, to the extent a cell phone search would be necessary to protect against a danger to officers, the warrantless search could be justified under the general exigency exception. *See, e.g.*, *Warden* v. *Hayden*, 387 U.S. 294 (1967).

support allowing warrantless cell phone seizures to preserve evidence.

First, from a financial standpoint, Faraday devices are very inexpensive. Top-of-the-line Faraday bags that can also be used for forensic evaluation cost only $58. Simpler Faraday envelopes can be purchased for only $6.95. And a sheet of aluminum foil costs only pennies. *See supra* at pp. 7-8.

Second, there would be no logistical burden on most law enforcement officers. Having a few small Faraday envelopes or a few sheets of aluminum foil in a squad car is not a significant burden. Indeed, a square foot of aluminum foil is lightweight and can be folded small enough to fit easily into a pocket or glove compartment. Moreover, few law enforcement officers would need to carry the Faraday envelope or aluminum foil with them. Even though the DEA, FBI, and local police officers working in drug or gang units might need immediate access to Faraday envelopes or aluminum foil, the average officer on the street is unlikely to encounter a situation in which it is essential to immediately preserve cell phone data.[9] Thus, the Faraday envelopes and

---

[9] A sizeable number of cell phone searches are conducted by a relatively small number of specialized law enforcement agencies. *See, e.g., U.S.* v. *Finley*, 477 F.3d 250 (5th Cir. 2007) (joint operation involving DEA); *U.S.* v. *Stephens*, No. 13-200004, 2013 WL 5409907 (W.D. Tenn. Sept. 25, 2013) (Organized Crime Unit of local police department); *U.S.* v. *Saldago*, No. 1:09-CR-454, 2010 WL 3062440 (N.D. Ga. June 12, 2010) (DEA agents); *U.S.* v. *LaSalle*, No. 07-00032, 2007 WL 1390820 (D. Haw. May 9, 2007) (DEA agent); *U.S.* v. *Brookes*, No. CRIM2004-0154, 2005 WL 1940124 (D. V.I. June 16, 2005) (DEA agents); *U.S.* v. *Cote*, No. 03CR271, 2005 WL 1323343 (N.D. Ill. May 26, 2005) (FBI agents); *U.S.* v. *Parada*, 289 F. Supp.2d 1291 (D. Kan. 2003) (DEA agents); *Wisconsin* v.

aluminum foil can be kept at the police station or in the officers' cruiser.

In its petition for certiorari in *U.S. v. Wurie*, the United States implicitly conceded that warrantless cell phone searches incident to arrest are a concern only in narcotics trafficking cases. Under the section heading, "The Question Presented Is Recurring And Important," the United States focused exclusively on the need for law enforcement officers to preserve evidence in complicated drug trafficking conspiracies. *See* Petition for Writ of Certiorari at *24-25, *U.S.* v. *Wurie*, No. 13-212 (Aug. 15, 2013), 2013 WL 4404658.

When specialized officers—such as DEA or FBI agents—conduct planned operations to interrupt a drug trafficking conspiracy, it makes sense that they carry Faraday envelopes or aluminum foil in their police cruisers so that they can prevent remote wiping by conspirators.

Most ordinary police officers on the street are not foiling complicated drug-trafficking operations. Ordinary police officers doing routine police work can bring cell phones to the police station where the phones can be placed in a Faraday envelopes or aluminum foil with no logistical difficulty.

Indeed, numerous cell phone search cases decided over the last five years demonstrate that it is already very common for police officers to bring cell phones to the station *prior to* searching them. *See, e.g., U.S. v. Wurie*, 728 F.3d 1, 2 (1st Cir. 2013) (explaining that phone was not searched until ten to

---

Carroll, 778 N.W.2d 1 (Wis. 2010) (drug task force agent).

fifteen minutes after being taken to the police station).[10] Faraday envelopes and aluminum foil can thus be stored at the station, and the Seventh Circuit's concern that disallowing warrantless cell phone searches would place a "burden on the police of having to traipse about with Faraday bags" is misplaced. *See Flores-Lopez*, 670 F.3d at 810.

---

[10] *See also U.S.* v. *Murphy*, 552 F.3d 405 (4th Cir. 2009) (seized cell phones were brought to Virginia State Police headquarters and later turned over to the DEA); *U.S.* v. *Gholston*, No. 13-20187, 2014 WL 279609 (E.D. Mich. Jan. 27, 2014) (FBI agent seized cell phone and then submitted an application for a warrant); *U.S.* v. *Dixon*, No. 1-12-CR-205, 2013 WL 4718934 (N.D. Ga. Sept. 3, 2013) (ATF agent searched phone at office); *U.S.* v. *Nyuon*, No. CR.12-40017-01, 2013 WL 943635 (D.S.D. Mar. 11, 2013) (drug task force officer searched cell phone at station); *U.S.* v. *Dimarco*, No. 12CR205, 2013 WL 444764 (S.D.N.Y. Feb. 5, 2013) (search of cell phone at station six hours after arrest); *U.S.* v. *Wall*, No. 08-60016, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008) (DEA agents searched cell phone at station); *U.S.* v. *Rocha*, No. 06-40057-01, 2008 WL 4498950 (D. Kan. Oct. 2, 2008) (search by DEA task force agent at station); *U.S.* v. *James*, No. 1:06CR134, 2008 WL 1925032 (E.D. Mo. Apr. 29, 2008) (search "several days after the cell phone was seized" under the automobile exception); *U.S.* v. *Park*, No. CR05-375, 2007 WL 1521573 (N.D. Cal. May 23, 2007) (phones were taken to police station and "placed into envelopes for safe keeping"); *California* v. *Diaz*, 244 P.3d 501 (Cal. 2011) (search of cell phone 90 minutes after arrestee brought to police station); *Connecticut* v. *Boyd*, 992 A.2d 1071 (Conn. 2010) (search of cell phone "[l]ater that night" at the police station); *Ohio* v. *Smith*, 920 N.E.2d 949 (Ohio 2009) (explaining that search of cell phone likely occurred at police station); *Gracie* v. *Alabama*, 92 So.3d 806 (Ala. Crim. App. 2011) (search of cell phone at station); *Oregon* v. *Nix*, 237 P.3d 842 (Or. Ct. App. 2009) (cell phone transported to police station so that it could be analyzed by an agent specially trained in cell phones).

Finally, if an officer is not near the police station, she can request backup from another police officer who has a Faraday envelope or aluminum foil in his patrol car. *See, e.g.*, *U.S.* v. *Curry*, No. 07-100, 2008 WL 219966, at *2-3 (D. Me. Jan. 23, 2008) (explaining how DEA agent seized cell phones until another officer brought an evidence storage bag to the scene).

In sum, even though it might be wise for specialized groups of law enforcement agents—such as DEA and FBI agents—to be equipped with Faraday envelopes or aluminum foil, the vast majority of police officers would not have to carry either item. The cost and logistical difficulty of Faraday envelopes or aluminum foil is therefore minimal.

2. There is ample precedent to support a rule that police can seize cell phones and place them in Faraday envelopes, but not conduct searches of the devices without a warrant. In at least three contexts—seizure of individuals, seizure of evidence, and searches of automobiles—the Court has encouraged police to conduct warrantless seizures in order to prevent destruction of evidence so that officers can obtain a warrant before searching.

Seizure of Individuals: The Court has encouraged law enforcement to immobilize individuals who might destroy evidence inside of a home while the officers apply for a warrant. In *Illinois* v. *MacArthur*, 531 U.S. 326 (2001), the Court approved the warrantless seizure of an individual to prevent him from entering his home and destroying evidence while the police waited for a magistrate to issue a warrant.

There, police had probable cause to believe MacArthur had marijuana in his house, but they lacked a warrant to enter. *See id.* at 328. Rather than entering and searching without a warrant, the officers restricted MacArthur's movements and prevented him from entering the residence unsupervised for a period of two hours while they applied for a warrant. *See id.* at 329. MacArthur moved to suppress the marijuana and related contraband on the ground that the police had seized him unlawfully. *See id.* The Court rejected MacArthur's challenge to the seizure, concluding that the police acted reasonably by taking a far less invasive action than a warrantless search. *See also Segura* v. *U.S.*, 468 U.S. 796 (1984) (despite splitting on legality of a search, the majority and minority both recognized that it would have been far less invasive for police to seal the residence from the outside without a warrant, than to search without a warrant).

Seizure of Evidence: The Court has likewise approved of warrantless seizure of tangible items while the police procure a warrant to search them. In *U.S.* v. *Place*, 462 U.S. 696 (1983), police had reasonable suspicion that a traveler who had just landed at LaGuardia Airport had drugs in his suitcases. When Place refused to consent to a search of the luggage, officers seized the suitcases and took them across town to Kennedy Airport where a drug-sniffing dog alerted that drugs were in at least one of the suitcases. Place moved to suppress on the grounds that the police could not seize his luggage without a warrant. Although the Court ultimately concluded that the detention of the luggage was too lengthy to comply with *Terry* v. *Ohio*, 392 U.S. 1

(1968),[11] the Court recognized that it was permissible for police to seize the luggage to pursue further investigation but not search it without a warrant. Once again, the Court recognized that there are varying levels of intrusiveness and that a seizure of items such as luggage is less invasive than warrantless searching. *See id.* at 705-06. *See also U.S.* v. *Chadwick*, 433 U.S. 1, 15 n.8 (1977) (finding warrantless search of a footlocker unconstitutional, and noting that "[a] search of the interior was therefore a far greater intrusion into Fourth Amendment values than the impoundment of the footlocker").

Containers in Automobiles: For a short time, the Court required police with probable cause for a specific container in an automobile to seize the container, but not search it without a warrant. Even though the Court ultimately abandoned this rule, it did so because of peculiarities in the automobile context that would not be present with respect to cell phones.

In *Arkansas* v. *Sanders*, 442 U.S. 753 (1979), officers had probable cause to believe that a suitcase placed in the trunk of a taxi contained marijuana. The police thus had probable cause for a container in a vehicle, but not the vehicle itself. The Court refused to uphold a warrantless search of the suitcase, concluding that the police should have seized the suitcase without a warrant but procured a search warrant before opening it. The Court focused

---

[11] The duration problem would not be present in the cell phone context because the searches would be incident to arrest, rather than under the more limited *Terry* doctrine at issue in *Place*.

on the privacy associated with luggage and explained that "luggage is a common repository for one's personal effects, and therefore is inevitably associated with the expectation of privacy." *Id.* at 762.

The Court ultimately overruled *Sanders* in *California* v. *Acevedo*, 500 U.S. 565 (1991) for two reasons. First, requiring containers to be seized but not searched without a warrant was too confusing for police who had to make quick decisions in the automobile context. *See Acevedo*, 500 U.S. at 576. The rule in *Sanders*—that police had to obtain a warrant when they had probable cause solely for a container that happened to be in a vehicle—caused confusion given that the automobile exception allows police to search anything in a vehicle when they have probable cause for the vehicle itself. *See U.S.* v. *Ross*, 456 U.S. 798 (1981). Second, this confusion came with negligible benefit because, as the Court recognized in *Sanders* and reiterated in *Acevedo*, "Since the police . . . have probable cause to seize the property, we can assume that a warrant will be routinely forthcoming. . . ." *Acevedo*, 500 U.S. at 575 (quoting *Sanders*, 442 U.S. at 70). In short, the rule that police had to seize, but not search a container in a vehicle, was difficult to apply with respect to automobiles and added little privacy protection.[12]

---

[12] Notably, the *Acevedo* Court did not disturb the rule that outside of the automobile context police could seize a container but would not be permitted to search it without a warrant. *See* Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1441 (2010).

Neither of these problems would be present in the cell phone context. First, a rule that police can seize a cell phone incident to arrest but not search the phone without a warrant is perfectly clear. Following a lawful arrest, officers will know that they may seize a cell phone and place it in a Faraday envelope, but that they cannot search it without a warrant. There is no room for ambiguity.

Second, unlike in *Sanders*, a bright-line rule allowing warrantless seizures—but not searches—of cell phones incident to arrest would be very protective of privacy. When police seize a cell phone following an arrest, a warrant will not "be routinely forthcoming." *Acevedo*, 500 U.S. at 575 (quoting *Sanders*, 442 U.S. at 70). Even though there may be probable cause for an arrest, that would not usually mean there would be probable cause to believe an arrestee's cell phone contains evidence of a crime. Additionally, even if there were probable cause that some application on the phone might contain evidence, a magistrate could conclude that there is only probable cause for particular applications on the phone—for instance, the text messages—and therefore authorize a search only of that application. *See* Gershowitz, *Seizing a Cell Phone Incident to Arrest*, *supra*, at 611 (noting that magistrates are free to issue warrants that limit which applications and functions police can search). Requiring police to procure a warrant will therefore limit the search to locations on the phone where evidence is likely to be, rather than allowing general rummaging through text messages, email, photos, internet browsing history, and other private data that also happens to be on the phone.

B. The Court Should Not Apply *Arizona* v. *Gant*'s "Reasonable To Believe" Stand-ard To Cell Phones.

This Court should reject the conclusion of a few lower courts and scholars that the *Arizona* v. *Gant*, 556 U.S. 332, 343 (2009), "reasonable to believe" formulation should be applied to cell phone searches incident to arrest because it would allow widespread warrantless searches following arrests for minor offenses. The *Gant* standard would not impose a meaningful limitation on law enforcement because it could be reasonable for police to believe evidence of numerous minor offenses might be found on the phone.

In *Gant*, the Court narrowed *New York* v. *Belton*, 453 U.S. 454 (1981) by permitting searches of vehicles incident to arrest only when the arrestee is unsecured or when it is "reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle." *Gant*, 556 U.S. at 343 (quoting *U.S.* v. *Thornton*, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)).

In narrowing the search incident to arrest doctrine, the *Gant* Court recognized the need to prevent wide-ranging searches following arrests for minor offenses. The Court explained that there was a widespread privacy risk in allowing container searches:

> [S]earches [under the old rule in *Belton*] authorize police officers to search not just the passenger compartment but every purse, briefcase, or other container within that space. A rule that gives police the power to conduct such a search whenever an individual is

> caught committing a traffic offense, when there is no basis for believing evidence of the offense might be found in the vehicle, creates a serious and recurring threat to the privacy of countless individuals. Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects.

Id. at 345.

A few courts and scholars have maintained that applying the *Gant* "reasonable to believe" formulation to cell phone searches would protect against invasive searches following arrests for minor offenses. *See, e.g.*, *U.S.* v. *McGhee*, No. 8:09CR31, 2009 WL 2424104, at *3 (D. Neb. July 21, 2009); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 406-07 (2013). This is not correct.

Because of the enormous quantity and wide variety of information held in cell phones, it could be reasonable for police to believe evidence of many minor crimes might be found on cell phones. Applying the *Gant* standard to cell phone searches incident to arrest would thus fail to achieve the goal of preventing police officers from having "unbridled discretion to rummage at will among a person's private effects." *Gant*, 556 U.S. at 345.

A few low-level offenses are illustrative.

Drunk Driving: Driving while intoxicated is one of the most common criminal offenses committed in

the United States, with nearly 1.5 million arrests annually.[13] Many cell phones now have applications that enable users to pay their bills by using their phones.[14] One application—Google Wallet—is now accepted as a method of payment in "hundreds of thousands of merchant locations in the United States."[15]

Because Google Wallet and other cell phone applications can hold a receipt documenting the location where alcohol was consumed, the time a bar tab was paid, and the specific alcoholic drinks purchased, it is "reasonable to believe" evidence of the crime of drunk driving might be found on the phone.

Additionally, given the frequency with which people photograph themselves in social situations, it could also be reasonable for police to believe photographic evidence of a night of drinking might be found in the photo library of a cell phone. The *Gant* formulation would thus permit searches incident to arrest of photo galleries and any applications that my contain photos, such as Twitter, Facebook, and Instagram following a drunk driving arrest.

---

[13] *See* CRIMINAL JUSTICE INFO. SERVS. DIV., U.S. DEP'T OF JUSTICE, TABLE 29: ESTIMATED NUMBER OF ARRESTS (2009), http://www2.fbi.gov/ucr/cius2009/data/table_29.html.

[14] *See* Laurie Segall, *5 Pay-By-Phone Apps Tested*, CNNMONEY (Sept. 24, 2012, 9:31 AM), http://money.cnn.com/gallery/technology/2012/09/24/mobile-payment-apps/index.html.

[15] *See Frequently Asked Questions*, GOOGLE WALLET, http://www.google.com/wallet/faq.html (last visited Mar. 4, 2014).

Texting While Driving: Many jurisdictions criminalize texting while driving or other types of distracted driving, such as operating a vehicle while "[m]anually entering multiple letters or text in the device as a means of communicating with another person." N.C. GEN. STAT. ANN. § 20-137.4A; *see* Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 ARIZ. L. REV. 577 (2012) (summarizing all state statutes). And even though most jurisdictions punish texting while driving and other distracted driving with only a small fine, minor traffic offenses are arrestable offenses in many jurisdictions. *See* Janet Koven Levit, *Pretextual Traffic Stops:* United States *v.* Whren *and the Death of* Terry *v.* Ohio, 28 LOY. U. CHI. L.J. 145, 152 nn.63-64 (1996) (minor traffic offenses are arrestable offenses in many jurisdictions). As such, police in many states are authorized to conduct a search incident to arrest following an arrest for texting while driving. *See Atwater* v. *City of Lago Vista*, 532 U.S. 318, 354 (2001).

If an officer arrests an individual for texting while driving, it would obviously be reasonable for the officer to believe evidence of the texting might be found on the driver's cell phone. But the officer would not be limited to reviewing text messages. In states that forbid "manually entering multiple letters or text in the device as a means of communicating" while driving, *e.g.*, N.C. GEN. STAT. ANN. § 20-137.4A, it would be reasonable for the officer to search, at minimum, any text messages, email messages, internet browsing history, Facebook accounts, or other social media applications on the phone for

evidence that the phone was in use while driving. Under the *Gant* rationale, officers would therefore be justified in conducting wide-ranging searches of cell phones for low-level traffic offenses that carry only a small fine. *See, e.g.*, MASS. GEN. LAWS ANN. ch. 90, § 13B (punishing texting while driving with a $100 fine); N.J. STAT. ANN. § 39:4-97.3 ($100 fine); N.C. GEN. STAT. ANN. § 29-137.4A ($100 fine); R.I. GEN. LAWS § 31-22-30 ($85 fine); TENN. CODE ANN. § 55-8-199 (fine of no more than $50); WYO. STAT. ANN. § 346.89 (up to $75 fine).

Low Level Drug Possession: The *Gant* formulation could also permit police to search cell phones incident to arrest following arrests for possession of a small amounts of drugs, such as marijuana.

Drug purchases are often coordinated by text message. *See, e.g.*, *U.S.* v. *Aguirre*, 664 F.3d 606, 615 (5th Cir. 2011) (noting testimony of FBI agent that cell phones record evidence of the "buying and selling of drugs"); *U.S.* v. *Finley*, 477 F.3d 250, 254 n.2 (5th Cir. 2007) (describing incriminating text messages in search incident to arrest of cell phone). Because law enforcement is aware that texting is a way to conduct drug transactions, officers are trained to search cell phones in drug arrests. *See U.S.* v. *Wall*, No. 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008) (quoting testimony of drug enforcement agent that "it is his practice to search cell phones for text messages primarily because DEA's policy allows for it and because it is common to find text messages that further the investigation").

An officer who arrests a suspect for possession of a small amount of marijuana may reasonably believe

the purchase was coordinated by text message or other social media communication, thus authorizing a search of the phone under the *Gant* formulation. An arrest for a small amount of marijuana could therefore permit a wide-ranging search of the phone's text messages, emails, or Facebook messages.

Because police conduct thousands of arrests for minor narcotics possession each year,[16] the *Gant* formulation would authorize police to search cell phones incident to arrest following an enormous number of low-level drug possession arrests.

Any offense in which location data proves guilt: Perhaps most significantly, applying the *Gant* standard to cell phone searches incident to arrest would authorize police to search cell phones incident to arrest for any crime where a suspect's location could help to prove his guilt.

Cell phones contain an enormous amount of location data that can link an individual to minor criminal activity. Some cell phones contain a history function that documents every location where the phone has been for multiple weeks.

On iPhones with new operating systems, a police officer simply has to tap the "Settings" icon, then "Privacy," followed by "Location Services," then "System Services," and finally "Frequent Locations." The iPhone will then show the addresses where the phone has been over the last few weeks. And if the

---

[16] *See, e.g.*, N.Y. STATE DIV. OF CRIMINAL JUSTICE SERV., ADULT ARRESTS: 2003-2012, http://www.criminaljustice.ny.gov/crimnet/ojsa/arrests/Allcounties.pdf (noting 62,115 to 83,758 misdemeanor drug arrests annually in New York City alone).

officer taps on a particular address, the iPhone will specify the exact dates and times when the phone was present at that location. *See* Dwight Silverman, *Your iPhone Knows Where You've Been, Puts It on a Map*, SEATTLE POST-INTELLIGENCER, Oct. 31, 2013, http://blog.chron.com/techblog/2013/10/your-iphone-knows-where-youve-been-puts-it-on-a-map/.

Older phones and less sophisticated models also contain functions or applications that include location data. The map function on many cell phones can provide law enforcement with the specific addresses where an individual has recently traveled. The Foursquare check-in application can automatically record when a phone has been near a specific business.[17]

In light of the vast location data stored on cell phones, it is reasonable for law enforcement to believe evidence of many minor crimes might be found on the phone. For example, following a prostitution arrest, officers might reasonably believe the cell phone could link the arrestee to an incriminating address. In an arrest for petty theft, the phone might show that the arrestee was at the store when the theft occurred. In an arrest for public intoxication or underage drinking, the phone might prove presence at a bar or on a public street.

In all of these examples—driving while intoxicated, texting while driving, minor drug possession, prostitution, petty theft, public intoxication, and underage drinking—the phones

---

[17] *See* MG Siegler, *Check-in on Foursquare Without Taking Your Phone Out of Your Pocket*, TECHCRUNCH, Aug. 2, 2010, http://techcrunch.com/2010/08/02/future-checkin/.

might contain evidence that links individuals to criminal activity. The problem is not this incriminating evidence. The problem is the reams of unrelated private information—voicemail and text messages from spouses or lovers, health records, embarrassing photographs, business documents, and future travel plans—that law enforcement officers will be able to review after arresting an individual for a minor crime. *See* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 41-44 (2008) (detailing the sensitive and embarrassing information an officer can come across during a search incident to arrest of a cell phone).

Moreover, allowing searches of cell phones under the *Gant* formulation would invite abuse. It is not far-fetched to imagine a police officer, after pulling someone over and arresting him for texting while driving, to suspect that he may have committed other crimes based on his look, the location, or even the time of day. The officer could then arrest the suspect for texting while driving and rummage through any text messaging application looking for evidence of other crimes the officer has a hunch the driver may have committed.

As technology advances, the list of minor offenses that could give rise to an invasive cell phone search under the *Gant* formulation will almost certainly grow. As time and technology move forward, the *Gant* formulation will therefore provide less and less protection against general police rummaging of cell phones. Accordingly, the Court should reject the *Gant* formulation in specifying the scope of a search incident to arrest of cell phones.

* * *

A bright-line rule permitting seizures, but not searches, of cell phones incident to arrest would in no way injure law enforcement's ability to preserve evidence. Should law enforcement choose to use a Faraday envelope or aluminum foil, that approach would be both workable for the police and protective of the reams of private data stored on or accessible from cell phones. And as the Court explained in *Segura*, "a seizure affects only possessory interests, not privacy interests. Therefore, the heightened protection we accord privacy interests is simply not implicated where a seizure of premises, not a search, is at issue." 468 U.S. at 810. Thus, the rule finds the right balance between protecting the government's evidence preservation interest and the citizen's privacy interest.

CONCLUSION

For these reasons, the judgment below should be reversed in *Riley* and affirmed in *Wurie*.

Respectfully submitted,

Adam M. Gershowitz
Professor of Law
WILLIAM & MARY
LAW SCHOOL

Patricia E. Roberts
WILLIAM & MARY LAW
SCHOOL APPELLATE AND
SUPREME COURT CLINIC
P.O. Box 8795
Williamsburg, VA 23187
Telephone: 757-221-3821

Tillman J. Breckenridge
(*Counsel of record*)
Tara A. Brennan
REED SMITH LLP
1301 K Street NW
Washington, DC 20005
Telephone: 202-414-9200
Facsimile: 202-414-9299
tbreckenridge@reedsmith.com

Counsel for Amici Curiae
Criminal Law Professors

Appendix

Gerald G. Ashdown
James H. Buck and June M. Harless Professor of Law
West Virginia University College of Law

Miriam H. Baer
Associate Professor of Law
Brooklyn Law School

Jeffrey Bellin
Associate Professor of Law
William & Mary Law School

Robert M. Bloom
Popeo Scholar and Professor of Law
Boston College Law School

Ronald Bretz
Professor of Law
Thomas M. Cooley Law School

John Burkoff
Professor of Law
University of Pittsburgh School of Law

Robert Calhoun
Professor of Law
Golden Gate School of Law

Bennett Capers
Professor of Law
Brooklyn Law School

Gabriel J. Chin
Professor of Law
University of California Davis School of Law

Brian Gallini
Associate Professor of Law
University of Arkansas School of Law

Adam M. Gershowitz
Professor of Law
William & Mary Law School

Stephen E. Henderson
Professor of Law
The University of Oklahoma College of Law

K. Babe Howell
Associate Professor of Law
CUNY School of Law

Alex Kreit
Associate Professor of Law
Thomas Jefferson School of Law

Lee Kovarsky
Associate Professor of Law
University of Maryland Francis King Carey School of Law

Nancy Leong
Assistant Professor of Law
University of Denver Sturm College of Law

Arnold H. Loewy
George Killam Professor of Criminal Law
Texas Tech School of Law

Michael J. Zydney Mannheimer
Professor of Law
Salmon P. Chase College of Law, Northern Kentucky University

Paul Marcus
Haynes Professor of Law
William & Mary Law School

Daniel Medwed
Professor of Law
Northeastern University School of Law

L. Song Richardson
Professor of Law
University of Iowa College of Law

Ira P. Robbins
Professor of Law & Barnard T. Welsh Scholar
American University Washington College of Law

Laurent Sacharoff
Associate Professor of Law
University of Arkansas School of Law

George C. Thomas III
Rutgers University Board of Governors Professor of Law
Judge Alexander P. Waugh, Sr. Distinguished Scholar
Rutgers Law School

Sandra Guerra Thompson
Alumnae College Professor of Law
University of Houston Law Center

Melanie D. Wilson
Professor of Law and Associate Dean for Academic Affairs
University of Kansas School of Law

Samuel R. Wiseman
Assistant Professor of Law
Florida State University College of Law

Jonathan Witmer-Rich
Assistant Professor of Law
Cleveland Marshall College of Law

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

No. 13-132

FILED
MAR 10 2014
OFFICE OF THE CLERK
SUPREME COURT, U.S.

IN THE
Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari to the Court of Appeal of California, Fourth Appellate District

---

BRIEF *AMICUS CURIAE* OF THE DKT LIBERTY PROJECT IN SUPPORT OF PETITIONER

Donald B. Mitchell, Jr.*
James H. Hulme
ARENT FOX LLP
1717 K Street, N.W.
Washington, DC 20036
(202) 857-6000
donald.mitchell@arentfox.com

*** Counsel of Record**

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

INTEREST OF *AMICUS CURIAE* 1

SUMMARY OF ARGUMENT 2

THE MODERN SMARTPHONE IS A SMALL COMPUTER IN WHICH CITIZENS HAVE EXTRAORDINARY PRIVACY INTERESTS 3

- The Smartphone is Ubiquitous. 3
- The Smartphone Is A Small Computer, And It Contains Intimate Information 4
- The Smartphone Is A Doorway Into The Home And A Repository Of Private Medical And Financial Papers 6
- The Smartphone Is A Window Into The Person's Mind 8
- Much Data Available To The Smartphone Is Not Actually Resident On The Device 11
- Once Seized, Smartphones Can Be Secured Until A Warrant Is Obtained 12

ARGUMENT 14

- The Fourth Amendment Protects Citizens' Privacy Interests In Their Smartphones 15
- Smartphones Have Been Recognized As A Doorway Into The Person, The Mind, And The Home. 20

Citizens Have A Reasonable Expectation Of Privacy In The Information On, Or Accessible By, Their Smartphones 25

Absent Exigent Circumstances, A Warrant Should Be Required To Search A Smartphone .. 28

CONCLUSION..... 35

TABLE OF AUTHORITIES

Page(s)

Cases

Arizona v. Gant,
556 U.S. 332 (2009) 29, 31

Arkansas v. Sanders,
442 U.S. 753 (1979) 18, 31

Boyd v. United States,
116 U.S. 616 (1886) 16

Brigham City v. Stuart,
547 U.S. 398 (2006) 30

Byars v. United States,
273 U.S. 28 (1927) 15

California v. Diaz,
244 P.3d 501 (Cal. 2011) 22

Chimel v. California,
395 U.S. 752 (1969) 29, 34

City of Ontario v. Quon,
560 U.S. 746 (2010) 25, 33

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 2, 15, 35

Dunaway v. New York,
442 U.S. 200 (1979) 32

Ex parte Jackson,
96 U.S. 727 (1877) 27

Illinois v. McArthur,
531 U.S. 326 (2001) 31

Johnson v. United States,
333 U.S. 10 (1948) 17

Katz v. United States,
389 U.S. 347 (1967) ..... passim

Kyllo v. United States,
533 U.S. 27 (2001) ..... passim

Lo-Ji Sales, Inc. v. New York,
442 U.S. 319 (1979) 25

McDonald v. United States,
335 U.S. 451 (1948) 18

Mincey v. Arizona,
437 U.S. 385 (1978) 35

Missouri v. McNeely,
133 S. Ct. 1552 (2013) 35

New York v. Belton,
453 U.S. 454 (1981) 23, 28, 32

Newhard v. Borders,
649 F. Supp. 2d 440 (W.D. Va. 2009) 5, 19

Ohio v. Smith, 920 N.E.2d 949 (Ohio 2009),
cert. denied, 131 S. Ct. 102 (2010) 24

Olmstead v. United States,
277 U.S. 438 (1928) 15, 33

Payton v. New York,
445 U.S. 573 (1980) 2, 19, 20

Schlossberg v. Solesbee,
844 F. Supp. 2d 1165 (D. Or. 2012) 22, 24, 32

Smallwood v. Florida,
113 So. 3d 724 ..... 21, 23, 26, 27

Texas v. Granville,
__ S.W.3d __, 2014 WL 714730 (Tex. Crim. App.
Feb. 26, 2014) 23, 31

Thornton v. United States,
541 U.S. 615 (2004) 32, 33

United States v. Chadwick,
433 U.S. 1 (1977) 3, 15, 19, 29

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) (en banc), cert. denied, 134 S. Ct. 899 (2014) 11, 21, 22, 24

United States v. Edwards,
415 U.S. 800 (1974) 23, 28

United States v. Finley,
477 F.3d 250 (5th Cir. 2007) 22

United States v Flores-Lopez,
670 F.3d 803 (7th Cir 2012) 14, 21

United States v. Park,
No. CR-05-375-SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007) 22, 23

United States v. Payton,
573 F.3d 859 (9th Cir. 2009) 27

United States v. Place,
462 U.S. 696 (1983) 4, 30, 31

United States v. Robinson,
414 U.S. 218 (1973) 23, 28

United States v. Tomero,
471 F. Supp. 2d 448 (S.D.N.Y. 2007) 14

United States v. Wurie,
728 F.3d 1 (1st Cir. 2013), cert. granted, No. 13-212 .....passim

Warden, Md. Penitentiary v. Hayden,
387 U.S. 294 (1967) 16

Weeks v. United States,
232 U.S. 383 (1914) 19

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 26

Constitutional Provisions

First Amendment 25

Fourth Amendment ..... passim

Other Authorities

Association of Chief Police Officers,
http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf 13

Black Hole Faraday Bag - RF Signal Isolation for Forensics, Standard Window Size,
http://www.amazon.com/Black-Hole-Faraday-Bag-Isolation/dp/B0091WILY0 14

A. Carrns, *More States Permit Digital Car-Insurance Cards*, New York Times (June 18, 2013),
http://bucks.blogs.nytimes.com/2013/06/18/more-states-permit-digital-car-insurance-cards/?_php=true&_type=blogs&_r=0 4

Cell Phone Activities 2013,
http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013 ..... 3, 8

S. Costello, *How Many Apps Are in the iPhone App Store*,
http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm 8

http://skjm.com/ 7

http://www.faradaybag.com 14

"iPeriod Period Tracker Free - Menstrual Calendar," https://itunes.apple.com/us/app/id340757216?mt=8 10

iTunes App Store, "Bathomatic," https://itunes.apple.com/us/app/bathomatic/id318150697?mt=8&ign-mpt=uo%3D4 7

iTunes App Store, "depressioncheck," https://itunes.apple.com/us/app/depressioncheck/id398170644 9

S. Kiume, *Top 10 Mental Health Apps*, http://psychcentral.com/blog/archives/2013/01/16/top-10-mental-health-apps/ 9

E. Landau, *Smartphone apps become 'surrogate therapists'* (Sept. 22, 2012), http://www.cnn.com/2012/09/27/health/mental-health-apps/index.html 9

LG 800G Prepaid Phone With Triple Minutes (Tracfone), http://www.amazon.com/LG-800G-Prepaid-Minutes-Tracfone/dp/B006E8MKZU/ref=sr_1_2?s=wireless 4

A. McCann, *Smartphone Shrink: 5 Apps To Help Your Mental Health*, http://www.popularmechanics.com/science/health/med-tech/smartphone-shrink-5-apps-to-help-your-mental-health#slide-1 9

Hon. M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 905 (2010) 19

Mobile Majority: U.S. Smartphone Ownership Tops 60%, http://www.nielsen.com/us/en/newswire/2013/mobile-majority--u-s--smartphone-ownership-tops-60-.html 3, 4

Nat'l Inst. of Standards and Tech., *Guidelines on Mobile Device Forensics*, Special Pub'n 800-101 (Draft, Sept. 2013), http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf 12

"Period Plus (Menstrual, Fertile, Ovulation, Calendar, Tracker, ... for Women Cycle)," https://itunes.apple.com/us/app/id318894849?mt=8 10

Push yourself further with Force™, http://www.fitbit.com/force 10

Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Mobile Phone Forensics*, (Feb. 11, 2013), https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20V2-0 13

The 64 Best Health and Fitness Apps of 2013 (Mar. 27, 2013), http://greatist.com/health/best-health-fitness-apps 10

Study Reveals Majority of Adults Share Intimate Details Via Unsecured Digital Devices, http://www.mcafee.com/us/about/news/2014/q1/20140204-01.aspx?culture=en-us&affid=0 5

U.S. Dep't of Justice, Criminal Division, Computer Crime and Intellectual Property Section (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf 21

S. Whitbourne, *Your Smartphone May Be Making You ... Not Smart* (Oct. 18, 2011), http://www.psychologytoday.com/blog/fulfillment-any-age/201110/your-smartphone-may-be-making-you-not-smart 6

INTEREST OF *AMICUS CURIAE*[1]

Thomas Jefferson warned "the natural progress of things is for liberty to yield and government to gain ground." Letter to Edward Carrington, May 27, 1788. Mindful of this trend, The Liberty Project was founded in 1997 to promote individual liberty against encroachment by all levels of government and to defend the right to privacy. The not-for-profit Liberty Project advocates vigilance over regulation of all kinds, especially restrictions of individual civil liberties that threaten the reservation of power to the citizenry that underlies our constitutional system. The Liberty Project has participated as *amicus* in this Court several times in the past, including in cases raising similar issues, such as *Kyllo v. United States*, 533 U.S. 27 (2001).

This case concerns the fundamental right of citizens to privacy in their papers and communications, and in their homes. The smartphone is a computer, small in size but full in function, creating and holding private papers, and providing access via the Internet to the home. Because of The Liberty Project's long interest in privacy and in protection of citizens from government overreaching, it is well situated to provide this Court with additional insight into the issues presented in this case.

---

[1] The parties have consented to the submission of this brief; their letters of consent are on file with the Clerk. None of the parties or their counsel authored this brief in whole or in part and no one other than *amicus* and its counsel contributed money or services to the preparation of this brief.

SUMMARY OF ARGUMENT

The modern smartphone is a miniaturized computer that creates content, sends mail, stores private papers, accesses personal financial and medical information, and runs computer programs to accomplish specific tasks. Notably, smartphones now enable remote access to the user's home. Smartphone users create such content and enable such access with the reasonable expectation that it will remain private.

1. The Fourth Amendment attaches when a citizen has a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347 (1967). The Court has recognized that the "reasonable expectation of privacy" standard evolves with technology and that the rules it adopts must take account of systems that are both in use or in development. *Kyllo v. United States*, 533 U.S. 27 (2001). A large quotient of judicial humility is called for when making rules involving evolving technology.

2. Searches conducted without prior approval by a magistrate are per se unreasonable under the Fourth Amendment, subject only to a few well-delineated exceptions. *Coolidge v. New Hampshire*, 403 U.S. 443 (1971). The exceptions are carefully drawn and the burden is on those seeking an exemption to show the need for it. *Id.* Absent exigent circumstances, the threshold of the home may not reasonably be crossed without a warrant. *Payton v. New York*, 445 U.S. 573 (1980). And *Kyllo* makes clear that a "virtual" search using technology that discerns activity within the home is forbidden by the Fourth Amendment.

3. The search incident-to-arrest exception to the Warrant Clause no longer applies once the property to be searched comes under the exclusive control of the police. *United States v. Chadwick,* 433 U.S. 1, 15 (1977). If the police have probable cause to believe that the smartphone contains evidence of the crime of arrest, they may seize the phone and turn it off or otherwise secure it so that there is no risk of destruction of evidence while a warrant upon probable cause is obtained. This simple standard comports with the needs of law enforcement for clear, bright line rules.

THE MODERN SMARTPHONE IS A SMALL COMPUTER IN WHICH CITIZENS HAVE EXTRAORDINARY PRIVACY INTERESTS

The Smartphone is Ubiquitous.

The modern smartphone[2] has become ubiquitous. Ninety-one percent of American adults own some form of mobile phone.[3] More than three out of five adult women use a smartphone,[4] and among persons between the ages of 25 and 34 about 78% own a

---

[2] Within the category of "smartphone" we also include the even newer technology commonly known as the "tablet" — they perform essentially the same functions.

[3] *Cell Phone Activities 2013*, http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013 (last accessed Mar. 3, 2014). All Internet sites cited in this brief were last accessed on March 3, 2014, and this date is not repeated in each citation below.

[4] *Mobile Majority: U.S. Smartphone Ownership Tops 60%*, http://www.nielsen.com/us/en/newswire/2013/mobile-majority--u-s--smartphone-ownership-tops-60-.html.

smartphone.[5] And the percentages of smartphone users are increasing. Thus, when police encounter an adult citizen, they are also likely to encounter a smartphone. The issues raised in this case, therefore, are widespread — and are only likely to become more frequent, significant, and prominent.[6]

The Smartphone Is A Small Computer, And It Contains Intimate Information

The modern smartphone is much more than a telephone. Even a $9.99 "Tracfone" can create content — it can record pictures and video, send and receive text messages, browse the Internet, etc.[7] And more sophisticated devices can create content, store papers, access personal financial and medical information, serve as a repository for thoughts, run computer programs to accomplish specific tasks, and store information and images that the creator does

---

[5] *Id.*

[6] About half the States now permit drivers to show police digital insurance cards on their smartphones to verify insurance at traffic stops. A. Carrns, *More States Permit Digital Car-Insurance Cards*, NEW YORK TIMES (June 18, 2013), *available at* http://bucks.blogs.nytimes.com/2013/06/18/more-states-permit-digital-car-insurance-cards/?_php=true&_type=blogs&_r=0. The future questions lurk: Has the citizen voluntarily given up his expectation of privacy in the phone? May the officer manipulate or search the phone? Does the "brief" nature of the phone seizure justify some search? *Cf., United States v. Place*, 462 U.S. 696, 705-06 (1983).

[7] *E.g., LG 800G Prepaid Phone With Triple Minutes (Tracfone)*, http://www.amazon.com/LG-800G-Prepaid-Minutes-Tracfone/dp/B006E8MKZU/ref=sr_1_2?s=wireless&ie=UTF8&qid=1393431740&sr=1-2&keywords=tracfone+cell+phones.

not intend others to view or see. It is not uncommon for adults to carry intimate photos of a spouse or romantic partner on the device, with no intention that others will view the photos. A recent survey by computer security company McAfee reports that a *majority* of mobile device owners have used them to "send or receive intimate content including video, photos, emails and messages;" among the eighteen to twenty-four year old group, the percentage sending or receiving intimate content was seventy percent.[8] And almost half of smartphone users have stored intimate content received from another person on their smartphones.[9]

Smartphone users create or save such intimate content with the expectation that it is private and will remain private. Yet, once the device is in the hand of the police, the photos or other private information are available to be viewed, passed around, and even shared with the public. This occurred in Virginia, where the police (without a warrant) found intimate photos of an arrestee's girlfriend in "sexually compromising positions" on the arrestee's phone and then alerted other officers in the station house and "members of the public 'that the private pictures were available for their viewing and enjoyment.'"[10]

---

[8] *Study Reveals Majority of Adults Share Intimate Details Via Unsecured Digital Devices*, http://www.mcafee.com/us/about/news/2014/q1/20140204-01.aspx?culture=en-us&affid=0.

[9] *Id.*

[10] *Newhard v. Borders*, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009).

The Smartphone Is A Doorway Into The Home And A Repository Of Private Medical And Financial Papers

The fully enabled smartphone has become an extension of one's self and a window into the person, her life, and her home.[11]

Smartphones are miniaturized computers. They operate by allowing their users to select and add what are commonly referred to as "apps" — software programs that implement a particular function[12] — to the base operating system. Common apps allow people to access their bank accounts to move money and make payments, access medical records, select and read newspapers, shop online, pay for on-street automobile parking, buy travel tickets, create and store information about their daily routines, and access other computers or other devices connected to computers, including computers and devices located in the home, far from where the phone user may be located.

For example, with one click of an icon on a smartphone one may literally look into the home (or other location) by using the "iCam" app to view an

---

[11] As one psychologist has noted, the "smartphone is quickly becoming an extension of the human brain." S. Whitbourne, *Your Smartphone May Be Making You ... Not Smart* (Oct. 18, 2011), http://www.psychologytoday.com/blog/fulfillment-any-age/201110/your-smartphone-may-be-making-you-not-smart.

[12] An "app" is "a self-contained program or piece of software designed to fulfill a particular purpose; an application, esp. as downloaded by a user to a mobile device." Google, "What is an app?".

Internet-connected camera installed in the home.[13] The most obvious use for these camera apps is to monitor your home. You can keep an eye on kids or pets while you are away, or keep an eye on the interior or exterior of the home when you are not there. Other home-related apps allow one to turn the lights and utilities on and off, monitor home security systems, and even prepare your bath, filling the bathtub to the homeowner's favorite combinations of temperature, depth and aroma.[14]

Other common services such as Google Docs and Apple's iWork allow one to create documents in the privacy of one's home or office and have them appear automatically on one's other devices — computers, smartphones and tablets — thus turning the mobile device into an extension of the home or office, a form of "digital home."

In addition to these uses, one can access confidential tax, banking, and investment records with the click of an icon on a smartphone. Almost thirty percent of smartphone users have used their device to check a bank balance or perform on-line

---

[13] The iCam app is available for iOS (Apple), Android, and Windows smartphones: http://skjm.com/.

[14] iTunes App Store, "Bathomatic," https://itunes.apple.com/us/app/bathomatic/id318150697?mt=8&ign-mpt=uo%3D4. In *Kyllo*, 533 U.S. at 38, this Court condemned technology that "might disclose ... at what hour each night the lady of the house takes her daily sauna and bath;" now, searching her Bathomatic-enabled smartphone, the Government will know not just the time but her favorite aroma and the depth of her bubbles.

banking functions.[15] A smartphone user can also view medical records and treatment history with just one or two clicks. In other words, almost every human activity can be documented, monitored, evaluated, and viewed on one's smartphone — no matter how personal, intimate or trivial. The Apple App Store now has more than one million "apps" for almost every conceivable human activity.[16]

As one uses a smartphone, a great deal of additional data about the person is created and stored. Photos taken by the device contain not just the image, but metadata such as where and when the photograph was taken. Every time an iPhone user closes the built-in mapping application, the phone stores a screenshot, thus memorizing where the phone was at that particular time. As various apps are opened and closed, data is created and stored about what apps were opened, how long they were open and, frequently, what was done on them. Access to this data can pinpoint the location of the device and a great deal about the private activities engaged in by the user.

The Smartphone Is A Window Into The Person's Mind

Just as the smartphone has become an extension of the home and an access point to financial and medical papers, it also has become a window into a person's mind, goals, failures and successes.

---

[15] *See Cell Phone Activities, supra* n.3.

[16] S. Costello, *How Many Apps Are in the iPhone App Store*, http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm.

Already, a smartphone owner may use the device as a surrogate therapist.[17] "Moody Me" is an app that allows the user to track his or her mental states. "You can delve deeper into what's causing the mood with a list of relevant emotions, symptoms and events. Users who are taking medications can also note them in their daily mood entries. The app also creates graphs of moods over time so users can detect patterns."[18] A person grappling with depression may consult "depressioncheck" — an app that "is a state-of-the-art, research validated screen that in 3 minutes assesses your risk of depression, bipolar and anxiety disorders (including PTSD). After completing the short checklist you receive a personalized confidential report sharing how much burden these symptoms may be causing you."[19] Other apps allow a user to track sleep, stress and relaxation levels.[20] The totality of these entries creates a record of the person's mind and its inner workings, his thoughts, her feelings. If viewed, the app data would be a look directly into the person's

---

[17] E. Landau, *Smartphone apps become 'surrogate therapists'* (Sept. 22, 2012), http://www.cnn.com/2012/09/27/health/mental-health-apps/index.html.

[18] *Id.*

[19] iTunes App Store, "depressioncheck," https://itunes.apple.com/us/app/depressioncheck/id398170644.

[20] *See, e.g.*, S. Kiume, *Top 10 Mental Health Apps*, http://psychcentral.com/blog/archives/2013/01/16/top-10-mental-health-apps/; A. McCann, *Smartphone Shrink: 5 Apps To Help Your Mental Health*, http://www.popularmechanics.com/science/health/med-tech/smartphone-shrink-5-apps-to-help-your-mental-health#slide-1.

mental state, feelings, and beliefs — information that is at the heart of the expectation of privacy.

One of the more common uses for apps is to assist the user with nutrition, physical fitness, and other health-related management activities. The "Fitbit" app allows the smartphone user to track "steps taken, distance traveled, calories burned, stairs climbed and active minutes throughout the day," and then at night to track sleep patterns, restless periods, and awake periods; all of the data are then stored, analyzed, and available to be displayed on the smartphone.[21] There are numerous apps that allow a woman to track and record her ovulation and menstruation cycle.[22] And there are thousands of apps and other devices which allow the user to record her daily activities, including the details of each meal eaten, beverages consumed, steps taken, each beat of the heart, etc.[23]

While most smartphone users (at least now) take advantage of only two or three dozen of the available apps, the most common uses often involve the most personal information. In a word, the smartphone is an extension of a person's papers — her financial records, his medical records — and a doorway into

---

[21] *Push yourself further with Force™*, http://www.fitbit.com/force.

[22] *E.g.*, "Period Plus (Menstrual, Fertile, Ovulation, Calendar, Tracker, ... for Women Cycle)," *available at* https://itunes.apple.com/us/app/id318894849?mt=8; "iPeriod Period Tracker Free - Menstrual Calendar," *available at* https://itunes.apple.com/us/app/id340757216?mt=8.

[23] *E.g.*, *The 64 Best Health and Fitness Apps of 2013* (Mar. 27, 2013), http://greatist.com/health/best-health-fitness-apps.

his or her mind, body, and home through the data stored or accessible on the device. It is, in many ways, nothing less than *home* — digital, but an extension of home nonetheless.

Much Data Available To The Smartphone Is Not Actually Resident On The Device

Smartphones have become so advanced and interconnected with the Internet that the data being viewed on the phone *is likely not even on the device.* Rather, by clicking on an icon, the user frequently causes the device to reach out to another computer to access and display the data, picture, etc. This other computer may be on what is commonly referred to as the "cloud."[24] *Or, it may be on or attached to another one of the user's computers in his or her home* — one that clearly could not be searched without a warrant. Just as clicking on the iCam icon causes the device to bring up a live-time view of whatever the remote camera is looking at, clicking on other icons may cause the device to display data that is actually stored on a remote computer.

Thus, a law enforcement officer examining a smartphone cannot tell whether he is inspecting the contents of the smartphone itself or, in reality, accessing a remote computer located in the owner's home or other location. Indeed, a police officer with access to the device who clicks the iCam icon will not

---

[24] "The term 'cloud computing' is based on the industry usage of a cloud as a metaphor for the ethereal internet...." *United States v. Cotterman,* 709 F.3d 952, 965 n.12 (9th Cir. 2013) (en banc), *cert. denied,* 134 S. Ct. 899 (2014).

know if he is about to peer into the home until the image appears on the screen.[25]

Once Seized, Smartphones Can Be Secured Until A Warrant Is Obtained

As soon as a smartphone is in the hands of the police, the arrestee cannot directly remove any data, and it may be secured until a warrant is obtained with no risk of loss of data or potential evidence.

Forensic specialists have reached a consensus as to the best methods to secure a smartphone once it has been seized. According to the National Institute of Science and Technology: "Two basic methods for isolating the mobile device from radio communication ... are to either place the device in airplane mode, turn the device off, or lastly place the device in a shielded container."[26] Forensic specialists in the United Kingdom agree: "Isolate the device from network – this may be achieved by one of the following techniques: Turn device off at the point of

---

[25] The United States, in its brief in *Wurie*, No. 13-212, concedes that the search incident-to-arrest "doctrine does not permit officers to use the phone's Internet connection to access files stored elsewhere." U.S. Br. at 10; *see also id.* at 43-44. The problem, as set forth in the text, is that the officer *cannot tell* that his search is actually accessing files stored elsewhere. Thus, for example, even email or voice mail accessed via a smartphone is usually not *on* the phone, but on the cloud.

[26] Nat'l Inst. of Standards and Tech., *Guidelines on Mobile Device Forensics*, Special Pub'n 800-101 (Draft, Sept. 2013), at 30, *available at* http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

seizure ... Place device in shielded container/bag."[27] Finally, the Scientific Working Group on Digital Evidence — which is chaired by representatives of the U.S. Secret Service and the FBI, and is composed of representatives of all federal law enforcement agencies — states: "If the phone is unable to be processed immediately, turn off phone, remove battery if practical, and do not turn it back on."[28] Tellingly, in its brief in *Wurie*, No. 13-212, the United States does *not* argue that turning the phone off does not preserve the data on it; instead, the United States argues that turning the phone off may mean that a password will be required to access its data, and that that would make law enforcement less convenient. *E.g.*, U.S. Br. in *Wurie*, at 34-37.

Thus, the simple and effective method of securing a smartphone is to turn it off. It may then be turned on in a secure location that is protected from outside interference, eliminating the threat of remote wiping. As noted above, another way to secure a device is to place it in a shielded container — a simple bag made of materials designed to prevent the device from communicating or being remotely wiped, generically

---

[27] *Good Practice Guide for Computer-Based Electronic Evidence (Official Release Version)*, Association of Chief Police Officers, at 46, *available at* http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf .

[28] *SWGDE Best Practices for Mobile Phone Forensics*, at 5 (Feb. 11, 2013), *available at* https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20V2-0.

called a "Faraday Bag."[29] Such bags are widely available at low cost for use on smartphones, tablets, laptops, and any other device that communicates over cellular, WiFi, satellite, or any other radio frequency network.[30] Once secured, any information on the device will be preserved until it may be forensically examined. In other words, once secured, the smartphone is no different from a desktop computer that is seized with a warrant on probable cause and held for a forensic examination.[31]

ARGUMENT

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures...." U.S. Const., amend. IV. "[T]he most basic constitutional rule in this area is that 'searches conducted ... without prior approval by judge or magistrate, are per se unreasonable under

---

[29] *See* http://www.faradaybag.com for but one source of such bags.

[30] *E.g., Black Hole Faraday Bag - RF Signal Isolation for Forensics, Standard Window Size,* http://www.amazon.com/Black-Hole-Faraday-Bag-Isolation/dp/B0091WILY0.

[31] It has been suggested, incorrectly, that turning a smartphone off does not really turn it off because it could contain a "roving bug" that would allow it to operate even when the device is "off." *E.g., United States v Flores-Lopez*, 670 F.3d 803, 808 (7th Cir 2012) (citing *United States v. Tomero*, 471 F. Supp. 2d 448, 450 & n.2 (S.D.N.Y. 2007)). The *Flores-Lopez* court misreads *Tomero*. In *Tomero*, the "roving bug" was a court-authorized wiretap installed by the FBI which made the phone's microphone constantly active as an area listening device.

the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions.'" *Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). "The exceptions are 'jealously and carefully drawn,'" and "'*[t]he burden is on those seeking the exemption to show the need for it.*'" *Id.* at 455 (emphasis added, footnotes and citations omitted).

The Fourth Amendment Protects Citizens' Privacy Interests In Their Smartphones

In his venerable and vindicated dissent in *Olmstead v. United States*, Justice Brandeis said that a constitutional provision such as the Fourth Amendment must have the "capacity of adaptation to a changing world." 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting). "In the application of a Constitution, therefore, our contemplation cannot be only of what has been but of what may be." *Id.* at 473 (citation omitted). *Accord United States v. Chadwick*, 433 U.S. 1, 9 (1977), *abrogated in part on other grounds, California v. Acevedo*, 500 U.S. 565 (1991) ("the Framers ... intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth").

In order to prevent the creeping loss of liberty about which Thomas Jefferson warned, *see* Interest of *Amicus Curiae, supra*, "Constitutional provisions for the security of person and property are to be liberally construed." *Byars v. United States*, 273 U.S. 28, 32 (1927). As Justice Bradley stated for the

Court in *Boyd v. United States*, 116 U.S. 616, 635 (1886):

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance.

The principles of the Fourth Amendment "apply to all invasions on the part of the government ... of the sanctity of a man's home *and the privacies of life.*" *Id.* at 630 (emphasis added). *Accord Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967) ("We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property....").

Thus it is black letter law that the Fourth Amendment attaches when a citizen has a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 351-52 (1967); *id.* at 360-61 (Harlan, J., concurring) ("there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

Crucially for this case, the Court has recognized that the "reasonable expectation of privacy" standard

evolves with technology. "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo,* 533 at 33-34.

> Reversing that [*Katz*] approach would leave the homeowner at the mercy of advancing technology.... While the technology used in the present case was relatively crude, *the rule we adopt must take account of more sophisticated systems that are already in use or in development.*

Id. at 35-36 (emphasis added).

The warrant requirement serves important and fundamental purposes, and abates the creeping loss of liberty otherwise inherent in the competitive activity of policing. Justice Jackson, speaking for the Court in *Johnson v. United States*, 333 U.S. 10 (1948), perhaps said it best:

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.... When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.

Id. at 13-14. *Accord Katz,* 389 U.S. at 358-59 ("bypassing a neutral predetermination of the scope

of a search leaves individuals secure from Fourth Amendment violations only in the discretion of the police") (citation and internal quotations omitted); *McDonald v. United States*, 335 U.S. 451, 455-56 (1948) ("The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.").

Good faith, good policing technique, and even actual probable cause do not excuse the requirement of a warrant.

> In the absence of [the judicial warrant procedure] safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," for the Constitution requires "that the deliberate, impartial judgment of a judicial officer ... be interposed between the citizen and the police."

Katz, 389 U.S. at 356-57 (citations omitted). *Accord Arkansas v. Sanders*, 442 U.S. 753, 758 (1979), *abrogated on its facts, California v. Acevedo*, 500 U.S. 565 (1991). As Chief Justice Burger stated for the Court:

> Once a lawful search has begun, it is also far more likely that it will not exceed proper bounds when it is done pursuant to a judicial authorization 'particularly describing the place

> to be searched and the persons or things to be seized.' Further, a warrant assures the individual whose property is searched or seized of the lawful authority of the executing officer ... and the limits of his power to search.

Chadwick, 433 U.S. at 9 (citation omitted).[32]

All of these Fourth Amendment concerns are sharpened and heightened when intrusion into the home is at issue, as is — and will increasingly be — the case with smartphone searches. Resistance to the British general warrants and writs of assistance "established the principle which was enacted into the fundamental law in the 4th Amendment, that a man's house was his castle, and not to be invaded by any general authority to search and seize his goods and papers." *Weeks v. United States*, 232 U.S. 383, 390 (1914); *accord Payton v. New York*, 445 U.S. 573, 597 n.45 (1980) ("'A man's house is his castle; and while he is quiet, he is as well guarded as a prince in his castle....'," *quoting* 2 Legal Papers of John Adams 142 (L. Wroth & H. Zobel eds. 1965)). *See generally* Hon. M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 905, 907-12 (2010).

> The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an

---

[32] The need for assurance of "proper bounds" and "the limits of his power to search" is exemplified by cases like *Newhard v. Borders*, *supra* n.11.

> individual's home — a zone that finds its roots in clear and specific constitutional terms: "The right of the people to be secure in their ... houses ... shall not be violated." ... [T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.

Payton, 445 U.S. at 589-90 (citation omitted). These principles apply, too, even to what some might consider a *de minimis* intrusion. *Kyllo*, 533 U.S. at 37 ("protection of the home has never been tied to measurement of the quality or quantity of information obtained" because "[i]n the home ... *all* details are intimate details, because the entire area is held safe from prying government eyes").

And *Kyllo* makes clear that even a "virtual" search — one using technology from outside the home that discerns activity within the home, like the thermal imaging device in that case — is forbidden by the Fourth Amendment. *Id.* at 40. All searches that access the privacy of the home without a warrant are forbidden, whether the police physically cross the threshold or enter the curtilage or not. *Id.* It does not matter the technology: Whether the technology is a telescope or thermal imaging — or the iCam app — the result is forbidden.

Smartphones Have Been Recognized As A Doorway Into The Person, The Mind, And The Home.

The U.S. Department of Justice readily acknowledges that "cell phones increasingly resemble

computers...."[33] Not surprisingly, virtually every court to address the issue has also found that modern smartphones combine features and have capabilities that previously would only be found in a library or office. *E.g., United States v Flores-Lopez*, 670 F.3d 803, 805 (7th Cir. 2012) ("a modern cell phone is a computer"); *Cotterman*, 709 F.3d at 964 ("Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails"); *Smallwood v. Florida*, 113 So. 3d 724, 732 (Fla. 2013) ("many people now store documents on their equipment that also operates as a phone that, twenty years ago, were stored and located only in home offices, in safes, or on home computers").

Modern smartphones have, for many people, effectively *replaced* desks and drawers and diaries, and contain or have access to the core secrets of their family, health, romantic, professional and financial lives that were formerly stored safely within the home — and which, undoubtedly, are subject to the warrant requirement when stored there. The First Circuit recognized this point in *United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013), *cert. granted*, No. 13-212, the companion case in this Court:

---

[33] *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. Dep't of Justice, Criminal Division, Computer Crime and Intellectual Property Section (2009), at 34 n.6, *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

> That information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records.... *It is the kind of information one would previously have stored in one's home and that would have been off-limits* to officers performing a search incident to arrest. *See Chimel [v. California]*, 395 U.S. 752 [(1969)].

(Emphasis added.) *See also Cotterman*, 709 F.3d at 964 ("This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.'"); *Schlossberg v. Solesbee*, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012) ("Electronic devices such as [a] digital camera hold large amounts of private information, entitling them to a higher standard of privacy."); *United States v. Park*, No. CR-05-375-SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) ("Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations").

Much ink has been spilled about whether smartphones are "containers" associated with an arrestee in a misguided (albeit understandable) effort to shoehorn this new technology into the search incident-to-arrest case law developed in the bygone days of paper, when a person could only bring with him the tangible property he could carry. *Compare, e.g., United States v. Finley*, 477 F.3d 250, 260 (5th Cir. 2007), and *California v. Diaz*, 244 P.3d 501, 507 (Cal. 2011) (each finding phone was a "container" and thus allegedly subject to search

under *New York v. Belton*, 453 U.S. 454 (1981)), *with United States v. Park*, 2007 WL 1521573, at *1 ("a modern cellular phone, which is capable of storing immense amounts of highly personal information, is properly considered a 'possession within an arrestee's immediate control' rather than as an element of the person"). But aside from the dubious *factual* determination that a smartphone would be a *Belton* container — since *Belton* states that a "container" is an "object capable of holding another object," 453 U.S. at 460 n.4, and a smartphone holds no "object" at all — the container analysis misses the *reality* of the technology and the constitutional privacy implications of citizens' uses of their smartphones.

The more recent decisions have begun to respect the *reality* that the nature of the smartphone means it cannot be shoe-horned into pre-digital boxes. *See, e.g., Smallwood*, 113 So. 3d at 732 ("the electronic devices that operate as cell phones of today are materially distinguishable from the static, limited-capacity cigarette packet in *Robinson*, not only in the ability to hold, import, and export private information, but by the very personal and vast nature of the information that may be stored on them or accessed through the electronic devices"); *id.* at 732-33 ("In our view, attempting to correlate a crumpled package of cigarettes to the cell phones of today is like comparing a one-cell organism to a human being.... The cell phones of today have a greater capacity not just in the *quantity* of information stored, but also in the *quality* of information stored"); *Texas v. Granville*, __ S.W.3d __, 2014 WL 714730, at *6 (Tex. Crim. App. Feb. 26, 2014) ("clothing [like in *Edwards*] does not contain private banking or medical information and records;

it does not contain highly personal emails, texts, photographs, videos, or access to a wide variety of other data about the individual citizen, his friends and family. Searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once"); *Cotterman*, 709 F.3d at 964 ("[t]he private information individuals store on digital devices — their personal 'papers' in the words of the Constitution — stands in stark contrast to the generic and impersonal contents of a gas tank"); *Schlossberg*, 844 F. Supp. 2d at 1169 ("[c]onsideration of an electronic device as a 'container' is problematic.... In order to carry the same amount of personal information contained in many of today's electronic devices in a container, a citizen would have to travel with one or more large suitcases, if not file cabinets"). *See also Ohio v. Smith*, 920 N.E.2d 949, 953-54 (Ohio 2009), *cert. denied*, 131 S. Ct. 102 (2010) ("The state argues that ... a cell phone is akin to a closed container and is thus subject to search upon a lawful arrest. We do not agree with this comparison").

And as technology has advanced, the devices have become even less like "containers." No longer do the devices simply "contain" information within them on an internal microchip — which is, after all, the underlying factual (and etymological) premise for the faulty "container" analogy. Instead, they now provide access via the "cloud" and Internet to other computers *not "contained" in the phone, and even to the home. See Wurie*, 728 F.3d at 8 ("modern cell phones provide direct access to the home....; iPhones can now connect their owners directly to a home computer's webcam, via an application called iCam"); *Cotterman*, 709 F.3d at 965 ("[t]he digital device is a

conduit to retrieving information from the cloud, akin to the key to a safe deposit box. Notably, although the virtual 'safe deposit box' does not itself [travel with its carrier or the phone], it may appear as a seamless part of the digital device.... With access to the cloud ... a traveler's cache is just a click away from the government"). It is as if Robinson's cigarette pack contained a key to his home or to a safety deposit box instead of capsules of heroin. No one would credibly argue that the police, having located the key, could simply use it to enter his home or safety deposit box without a warrant.

Citizens Have A Reasonable Expectation Of Privacy In The Information On, Or Accessible By, Their Smartphones

It is undisputed that citizens have a significant constitutional privacy interest in the contents within (on the chips of) their smartphones, *and* in their data and personal information on the cloud and other locations external to the phone that may be accessed remotely by those devices. As this Court recognized in *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010), "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."

The papers citizens store or access on their smartphones are often also expressive material, protected by First Amendment principles as well. As this Court has recognized, there are "special constraints upon searches for and seizures of material arguably protected by the First Amendment." *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 n.5 (1979). When searching First

Amendment protected areas, even searches *with* a warrant require special and careful limitation. *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). Such careful limitation is impossible in searches conducted by "competitive" police officers incident to arrest.

It is inconceivable that the privacy of the home, or a person's bank or financial or medical records — otherwise immune to seizure without a warrant — could be lost to Government merely by virtue of a citizen's use of the software and wireless amenities of modern life on a portable digital device. The devices are, after all, legal, and not themselves contraband. It is irrational that a person should lose constitutional protections available in the pre-digital world for her papers simply because technology now allows her to carry those papers, or a digital key to those papers, with her.[34] In this light, the devices are simply a *digital home*, or a digital extension of the home.

Each of the individual items of communications data commonly available on smartphones have been found to be entitled to protection in their pre-digital form. Over 100 years ago this Court recognized that private mail correspondence was constitutionally

---

[34] *Accord Smallwood*, 113 So. 3d at 738 ("allowing law enforcement to search an arrestee's cell phone without a warrant is akin to providing law enforcement with a key to access the home of the arrestee. Physically entering the arrestee's home office without a search warrant to look in his file cabinets or desk [on the one hand], or remotely accessing his bank accounts and medical records without a search warrant through an electronic cell phone [on the other], is essentially the same for many people in today's technologically advanced society").

protected under the Fourth Amendment even when the letter in question was placed in the public mail service. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection ... as if they were retained by the parties forwarding them in their own domiciles."). No different rule should apply to email simply because a person carries them on his smartphone.[35] Similarly, *Katz* recognized that voice communications were protected. *Katz v. U.S.*, 389 U.S. at 352. No different rule should apply to modern text messaging — frequently in practice a form of back-and-forth communication equivalent to a voice call — simply because a person chooses to use the keyboard on her phone instead of the mouthpiece in a phone booth to engage in that conversation. The typical computer and its Internet browsing history, too, are protected from search without a warrant. *See United States v. Payton*, 573 F.3d 859, 861-62 (9th Cir. 2009) (search of computer not expressly authorized by warrant is not a reasonable search). No different rule should compromise the privacy interest in a citizen's Internet activity simply because it occurs on a portable computer like a smartphone or a tablet instead of the desktop computer in one's home or office.

---

[35] The justices of the Florida Supreme Court observed that they, too, had privacy interests in the email accounts on their cell phones. *Smallwood*, 113 So. 3d at 733 ("Indeed, even justices on this Court routinely use cellular phones to access Court email accounts, and highly confidential communications are received daily on these electronic devices.").

A rule making smartphones freely searchable upon arrest would mean that any citizen committing an arrestable offense could have his most private papers and information viewed by the arresting officer without any prior judicial involvement. The Courts that wrote *Robinson, Edwards* and *Belton*[36] — all, notably, in the pre-digital era — could not have foreseen a world in which almost everyone would be carrying on their person an item containing their most personal papers and access to their home, rather than mere tangible physical evidence. Those cases should not be applied to searches of clearly distinct digital technology.

Absent Exigent Circumstances, A Warrant Should Be Required To Search A Smartphone

There is, in fact, no need to contort search incident-to-arrest law either to protect the government's interest in police safety and law enforcement or citizens' interests in protecting their reasonable expectation of privacy. In our view, proper application of the rationale that underlies the search-incident-to-arrest exception to the warrant requirement, and proper application of the cases themselves, easily resolves the issue in favor of respecting the citizen's reasonable expectation of privacy, and without harming the government's interest in law enforcement.

---

[36] *United States v. Robinson*, 414 U.S. 218 (1973); *United States v. Edwards*, 415 U.S. 800 (1974); *New York v. Belton*, 453 U.S. 454 (1981).

In *Chimel v. California*, 395 U.S. 752, 762-63 (1969), the Court held that the "principle" which "marks [the exception's] proper extent" is that "[w]hen an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons" and that "[i]n addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person *in order to prevent its concealment or destruction*." (Emphasis added.) *Accord Arizona v. Gant*, 556 U.S. 332, 339 (2009) (quoting *Chimel* and adding emphasis to *Chimel's* "in order to" clauses).

But when the circumstance that justifies this *exception to the general rule* that a warrant upon probable cause is always required disappears, so does the exception. "In our view, when no [other] exigency is shown to support the need for an immediate search, *the Warrant Clause places the line at the point where the property to be searched comes under the exclusive dominion of police authority.*" *Chadwick*, 433 U.S. at 15 (emphasis added). *Accord Gant*, 556 U.S. at 339 ("If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, *both justifications for the search-incident-to-arrest exception are absent* and the rule does not apply") (emphasis added). In *Gant*, the Court emphasized the need for "the scope of a search incident to arrest" to be "commensurate with its purposes." *Id.*

Thus, the obvious solution *when the police have probable cause to believe that the smartphone contains evidence of the crime of arrest* is for the police simply to seize the phone and turn it off or otherwise secure it so

that there is no risk of loss or destruction of evidence while a warrant upon probable cause is obtained.[37]

To be clear, the police may not seize all smartphones as a matter of course while they decide whether to seek a warrant to search the phone. They may seize a phone consistently with the Fourth Amendment only when they have *probable cause* (not just a reasonable suspicion) to believe that the phone contains evidence *of the crime of arrest*. The "probable cause" threshold for seizing the phone, even incident to arrest, is well-established. *See e.g., United States v. Place,* 462 U.S. 696, 701 (1983) ("[w]here law enforcement authorities have probable cause to believe that a container holds ... evidence of a crime, but have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if ... some other recognized exception to the warrant requirement is present," citing, *inter alia, Chadwick*). That probable cause

---

[37] Nothing about applying the usual Fourth Amendment rule and requiring a warrant in order to search smartphones incident to arrest would eliminate or modify the *alternative* "exigent circumstances" exception to the warrant requirement. For example, even though police may not search a home without a warrant, true exigency is an exception to that rule. *E.g., Brigham City v. Stuart,* 547 U.S. 398, 403-04 (2006) ("need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency"). We do not foreclose the possibility of a similar exigency exception for smartphones when, for example, it is believed that the smartphone contains information about the location of a kidnapped child, or may contain a triggering mechanism for a bomb.

standard recognizes the citizen's interest in continued possession of his smartphone and its monetary value. *Id.* at 706, 709-10 (specifically holding that the lesser "reasonable suspicion" standard justifies only a "brief" seizure of property, and that a seizure even for ninety minutes pending receipt of a warrant requires probable cause); *compare Illinois v. McArthur*, 531 U.S. 326, 334 (2001) (seizure with probable cause for two hours, pending arrival of warrant, permitted).[38] And *Gant* makes clear that it is "evidence relevant to the crime of arrest" that the police are entitled to search for, and that the search-incident-to-arrest exception does not authorize broad investigatory searches for evidence of *any* crime the arrestee might have committed. 556 U.S. at 343. *See also id.* ("In many cases, as when [the defendant] is arrested for a traffic violation, there will be no reasonable basis to believe the vehicle [or other property within the

---

[38] As a practical matter, if a custodial arrest is effected and the arrestee has the phone on his person when he is put into the police car or brought to the local jail, the phone may be *seized* and removed from his possession and inventoried on the same basis and under the same procedures as other property is taken from an arrestee during booking and incarceration. Even when properly seized at that time, however, it may not be *searched* without a warrant. *Sanders*, 442 U.S. at 766 ("Where ... the police ... lawfully have ... secured [arrestee's property], they should delay the search thereof until after judicial approval has been obtained."); *Texas v. Granville*, 2014 WL 714730, at *7 (search of cell phone after placement in jail property room requires warrant). But if the phone is not on the arrestee's person — for example, it is on the passenger seat or on his desk or nightstand or some other nearby location — it may only be seized with probable cause. *U.S. v. Place*, 462 U.S. at 701.

control of the arrestee, like a smartphone] contains relevant evidence.").

The simple standard proposed here — which we believe is required by the Fourth Amendment — also comports with the needs of law enforcement for clear, bright line, and practical rules. As this Court has repeatedly held, a "single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront." *Dunaway v. New York*, 442 U.S. 200, 213-14 (1979). This Court has therefore rejected both "inherently subjective and highly fact specific" rules that require "ad hoc determinations on the part of officers in the field" in favor of clear ones that will be "readily understood by police officers." *Thornton v. United States*, 541 U.S. 615, 623 (2004). *See also Belton*, 453 U.S. at 458 ("A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions ... may be literally impossible of application by the officer in the field"). Such a rule is especially called for in the digital device field. *Schlossberg*, 844 F. Supp. 2d at 1170 ("it is impractical to distinguish between electronic devices.... It would require officers to learn and memorize the capabilities of constantly changing electronic devices.").

A case-by-case approach allowing searches of some smartphone files or directories but not others based on the reasonableness of the individual officer's particularized inferences in any given case — for example, recent call logs are okay, but emails and iCam apps are not, while text messages depend on how recently they were sent or received — would

result in exactly the "inherently subjective and highly fact specific" set of rules the Court has warned against. *Thornton*, 541 U.S. at 623. Such a rule would be both extremely difficult for officers in the field to apply and open to questions of when the line has been improperly crossed and when protected information has been accessed. Of the two available simple rules — [1] seize the phone with probable cause and obtain a warrant to search it, or [2] search it every time without a warrant — the latter is quite obviously overbroad and inconsistent with Fourth Amendment interests.

A large quotient of judicial humility is called for when making rules about evolving technology, for if anything is clear it is that we cannot see the future nor foresee the digital (or other?) types of devices the minds of scientists will create. Citing its earlier errors, this Court recognized in *Quon*, 560 U.S. at 759, that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. *See, e.g., Olmstead v. United States*, 277 U.S. 438 (1928), overruled by *Katz v. United States*, 389 U.S. 347, 353 (1967)."

> Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations.... Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.

Id. See also United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring):

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. [Citation omitted.] This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. ... I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.

At bottom, the argument of California in this case (and of the United States in *Wurie*) fails because it allows the *Chimel* exception to swallow the Fourth Amendment warrant rule. Stripped of its legal verbiage, the United States's argument is both arrogantly dismissive of citizens' privacy interests[39] and based on expedience and convenience, neither of which justify circumventing the Warrant Clause. There is no true exigency in these cases once the police have possession of the smartphone. It is not a weapon, and the arrestee cannot destroy any evidence. And the over-hyped fear of "remote wiping" is "truly theoretical," *Wurie*, 728 F.3d at 11,

---

[39] *E.g.*, U.S. Br. in *Wurie*, at 3 (describing smartphones as "pervasive instrumentalities of crime"); *id.* at 30 (describing phones as "critical tools in the commission of crimes" that will "only become more useful in the commission of criminal offenses"). As Appellant's Brief points out in its first sentence, most people who are arrested are not "are never convicted of any crime" and are therefore not "criminals."

and nonexistent in the real world,[40] and can be obviated by two simple expedients: turn the phone off or put it in a shielded bag. *See also Wurie*, 728 F.3d at 11 (suggesting three options). The burden is on the Government, as the proponent of the exception to the warrant requirement, to demonstrate a *real* and exigent problem, not a "truly theoretical" possibility, that requires an exception to warrant requirement of the Fourth Amendment.[41] "[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." *Mincey v. Arizona*, 437 U.S. 385, 393 (1978).

CONCLUSION

For the reasons set forth above, we believe that warrantless cell phone data searches are *categorically* unauthorized under the search-

---

[40] It is notable that the brief of the United States in *Wurie*, No. 13-212, spends four pages, U.S. Br. at 37-41, discussing numerous hypotheticals about how a smartphone might be or could be remotely wiped, *yet fails to cite a single instance of remote wiping ever having actually occurred* after a smartphone was seized by the police. Given that "[t]he burden is on those seeking the exemption [from the Warrant Clause] to show the need for it, *Coolidge*, 403 U.S. at 455, the Government's failure to identify even a single instance of "remote wiping" actually occurring — especially after the First Circuit called out the threat as "truly theoretical" — is fatal to its effort to square smartphone searches with *Chimel's* rationale.

[41] Given the rapid speed with which warrants may now be obtained, *see Missouri v. McNeely*, 133 S. Ct. 1552, 1561-62 (2013) (noting that "telecommunications innovations" now "allow for the more expeditious processing of warrant applications"), the inconvenience and risk to law enforcement should be minimal.

incident-to-arrest exception. If the police have probable cause to believe that the smartphone contains evidence of the crime of arrest, they may seize the phone and turn it off or "bag it" so that there is no real risk of loss or destruction of evidence while a warrant upon probable cause is obtained.

Respectfully submitted,

Donald B. Mitchell, Jr.
James H. Hulme
ARENT FOX LLP
1717 K Street, N.W.
Washington, DC 20036
(202) 857-6000
donald.mitchell@arentfox.com

Dated: March 10, 2014

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

FILED
MAR 10 2014
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondents.

On Writ of Certiorari to the
California Court of Appeal, Fourth District

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND TWENTY-FOUR TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
GINGER MCCALL
ALAN BUTLER
DAVID HUSBAND
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

March 10, 2014

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF CONTENTS i

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 3

ARGUMENT 4

I. U.S. Consumers Are Dependent on Modern Cell Phones for a Wide Range of Personal and Business Activity 6

II. Modern Communications Providers Store Sensitive Personal Information on Remote Servers, Accessible to Authorized Users with Cell Phones, Tablets, and Other Devices 10

A. Mobile Apps Integrate Local and Remote Data to Provide Users With Access to Their Files and Communications 10

B. Mobile Apps Provide Access to Sensitive Information on Remote Servers 14

C. Cell phones Also Operate Much Like a Password, Providing Access to Remote Files and Information That Would Not Be Available to an Unauthenticated User 28

III. Law Enforcement Can Easily Mitigate the Risk of Cell Phone Data Loss Pending a Judicial Determination of Probable Cause 32

A. Standard, Low-cost Security Techniques Enable Law Enforcement to Significantly Reduce the Risk of Cell Phone Data Loss 33

B. Similar Security Procedures Have Already Been Adopted by Federal Agencies to Protect Sensitive Data in Other Contexts 39

CONCLUSION **44**

TABLE OF AUTHORITIES

CASES

Arizona v. Gant, 556 U.S. 332, 338 (2009) 4

Chimel v. California, 395 U.S. 752 (1969)..... 4, 5

United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) 32

United States v. Robinson, 414 U.S. 218 (1973)..... 4

OTHER AUTHORITIES

Aaron Smith, *Smartphone Ownership 2013*, PewResearch Internet Project (June 5, 2013.) 7

Aaron Smith, *The Best (and Worst) of Mobile Connectivity*, PewResearch Internet Project (Nov. 30, 2013) 8

Adamo Construction, Inc., *What is a SCIF or Sensitive Compartmented Information Facility?* (2014) 40

Amazon, *Cloud Drive Photos for iOS* (2014) 19

App Developer's Alliance, *The Growing App Market* (2012) 9

AppBrain, *Number of Available Android Apps in the Market* (2014) 13

Apple iCloud, https://www.apple.com/icloud/ (2014) 19

Apple Store Metrics 13

Apple, *iCloud Photo Sharing* (2014) 17

Apple, *iOS: Understanding Notifications* (2014) 13

Apple, *iPhone User Guide* 49 (2013) 11

Apple, *What is iOS 7* (2014) 11, 27

Association of Chief Police Officers, *Good Practice Guide for Computer-based Electronic Evidence* 48 (2008) 32, 33

AT&T, *What is a Smartphone?* (2014) 6

Bank of America, *Mobile Banking* (2014) 21

Bd. of Gov's of the Fed. Reserve Sys., *Consumer and Mobile Financial Services 2013* (Mar. 2013). 20, 21

Bluetooth Keyless, *FAQs About Passive Keyless Entry Mode* (2014) 29, 30

Box, *drchrono Description* (2014) 22

Box, https://www.box.com/ (2014). 19

Bruce Schneier, *Fatal Flaw Weakens RFID Passports*, Wired (Nov. 3, 2005) 39

Bruce Schneier, Opinion, *Does Big Brother Want to Watch?: Passport Radio Chips Send Too Many Signals*, N.Y. Times, Oct., 4, 2004 38

Cellbrite, *UFED TOUCH Ultimate: All-inclusive Mobile Forensic Solution* (2013) 36

Chase, *Mobile App* (2013) 21

Chuck Jones, *Apple's App Store to Hit 1 Million Apps*, Forbes (Dec. 11, 2013) 13

Citrix, *GoToMyPC: Remote Access Factsheet* (2013). 24

Citrix, *GoToMyPC: Total Mobility – Factsheet* (2013) 24

Comments of Electronic Privacy Information Center to State Dep't, Dkt. No. DOS-2006-0329 (2007) 37

Communication Technology Update and Fundamentals (August E. Grant & Jennifer H. Meadows eds., 2012). 10

ComScore, *2013 Mobile Future in Focus* (Feb. 22, 2013) 9

David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices For Use in Criminal Investigations*, Forensic Focus, Aug. 20, 2011 34

Deloitte Consulting, *mHealth: a Check-up on Consumer Use* (2014) 23

Deloitte Consulting, *Mobile Banking: A Catalyst for Improving Bank Performance* (2010) 20

Deloitte, *The State of the Global Mobile Consumer* (2013). 12

Dropbox, https://www.dropbox.com/ (2014) 19

Eamon P. Doherty, *Digital Forensics for Handheld Devices* (2013) 35, 36

El Paso Intelligence Center, *Tactical Intelligence Bulletin EB 11-09: Preserving Cell Phone Data* (2011) 32

Eli Goodman, *The Multi-Platform Majority: How Mobile is Changing the Way We Experience the Web*, comScore Blog (Dec. 9, 2013) 8

Elizabeth Stawicki, *Your Smartphone Might Hold Key to Your Medical Records*, Kaiser Health News (June 17, 2013) 22

Eoghan Casey & Benjamin Turnbull, *Digital Evidence on Mobile Devices*, in *Digital Evidence and Computer Crime* (2011) 30, 31

Evernote, *Keep Everything in Sync* (2014) 18

Facebook, *How do I log out of the iPhone or iPad App?* (2014) 28

Facebook, *Key Facts* (2014) 15

Fed. Commc'ns. Comm'n, *Mobile Wireless Competition Report (16th Annual)* (Mar. 21, 2013) 6

Full Slate, *Client Database* (2013) 18

General Electric, *GE Brillion Connected Appliances* (2014) 25

Goodwill Community Foundation, *What is the Cloud?* (2014) 12

Google Drive, https://drive.google.com (2014). 19

Google Play Store, *Flickr Application Page* (2014) 17

Google Play Store, *YouTube Application Page* (2014) 17

Google, *Android Quick Start Guide* 36 (2013) 11

Google, *Getting Started with IMAP and POP3* (2014) 14

Google, *Gmail Help: Open & Read Email* (2014) 14

Google, *Google Authenticator* (2014) 29

Google, *Sync Your Mail, Contacts, Calendar, and More* (2014 18

Greg Gogolin, *Digital Forensics Explained* (2013) 35

Jonathan Garro, *Mac Computer Skills: Unlock the Power of Your Mac's Keychain Utility*, Tuts+ (April 15, 2013) 27

Kit Eaton, *Apps to Protect Your Array of Passwords,* N.Y. Times, Oct. 17, 2013, at B10 28

Letter from Electronic Frontier Foundation, EPIC, Privacy Activism, Privacy Rights Clearinghouse, and World Privacy Forum to Legal Division Chief, Office of Passport Policy, Planning and Advisory Services, U.S. Dep't of State (April 4, 2005) 38

Lockitron, *Keyless Entry Using Your Phone* (2014). 30

Maeve Duggan, *Cell Phone Activities 2013,* PewResearch Internet Project (Sept. 19, 2013).. 6, 7

Matt McGee, *Google+ Hits 300 Million Active Monthly "In-Stream" Users, 540 Million Across Google,* Marketing Land (Oct. 29, 2013) ... 15

Media Fire, http://www.mediafire.com/ (2014)..... 19

Medisafe Project, MediSafe Meds & Pill Reminder, Google Play Store (2014) 23

Michal Wei et al., *Reliably Erasing Data From Flash-Based Solid State Drives,* 9th USENIX Conf. File & Storage Tech. (2011) 31

Molly Wood, *Phone, Meet the Tablet.,* N.Y. Times, Feb. 27, 2014, at B8 6

Nat'l Inst. of Stds & Tech, *Guidelines on Cell Phone Forensics,* Special Pub. No. 800-101 (May 2007) 34

Nest, *Learn More about the Nest App* (2014) 25

Nest, *Life with Nest Thermostat* (2014) 25

Nest, *Saving Energy* (2014) 26

Nest, *Smoke Co-Alarm, Inside & Out* (2014) 25

Paraben, *Wireless Stronghold Bags 2.0* (2013) 35

Peggy Anne Salz & Jennifer Moranz, *The Everything Guide to Mobile Apps* (2013) 12

Pei Zheng & Lionel Ni, *Smart Phones and Next Generation Mobile Computing* (2010) 10, 11

Phillip Inglesant & M. Angela Sassse, *The True Cost of Unusable Password Polices: Password Use in the Wild*, Proc. SIGCHI Conf. Hum. Factors Comp. Sys. (2010) 26

Rajini Vidyanathan, *Barack Obama's Top Secret Tent*, BBC News (March 22, 2011) 40

Ray Pun, *Adobe 2013 Mobile Consumer Survey: 71% of People Use Mobile to Access Social Media*, Adobe Digital Marketing Blog (July 25, 2013) 16

Rizwan Ahmed, Dr. Rajiv V. Dharaskar, & Dr. Vilas M. Thakare, *Digital Evidence Extraction and Documentation From Mobile Devices*, 2 Int'l J. Advanced Res. Comp. & Comm'n Eng. 1019 (Jan. 2013) 30

Rob LeFebvre, *Fetch or Push? Set Your E-mail Accounts to Maximize Battery Life, Speed of Delivery*, Cult of Mac (Aug. 5, 2013) 11

RSA, *RSA SecurID Authenticators: The Gold Standard in Two Factor Authentication* (2011) ... 29

Russell Kay, *Flash Memory*, ComputerWorld (June 7, 2010) 31

Statistic Brain, *Twitter Statistics* (Jan. 1, 2014) 15

Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.*, PewResearch Internet Project (Feb. 27, 2014) 7

Susannah Fox and Maeve Duggan, *Mobile Health 2012*, PewResearch Internet Project (Nov. 8, 2012) 22

Taconic System LLC, *Blood Pressure Monitor*, iTunes Preview (2014) 23

Tamtris Web Services Inc., *Fertility Friend*, iTunes Preview (2014) 23

The Fitbit Story (2014) 22

ThinkInsights, *Our Mobile Planet* *8*

Troy Hunt, *The Only Secure Password is the One You Can't Remember*, Lifehacker (Mar. 24, 2011) 26

Twitter, *How to Sign Out of Twitter for iPhone* (2014) 28

U.S. Dep't of State, *Bureau of Consular Affairs*. 39

Wells Fargo, *Mobile App* (2014) 21

What is Mint (2014) 21

Wi-Fi Alliance, *Connect Your Life: Wi-Fi and the Internet of Everything* (2014) 24

Windows Live OneDrive, https://onedrive.live.com/about/en-us/ (2014) 19

Yahoo!, *Privacy Policy: Flickr* (2014) 17

YouTube, *Video Privacy Settings* (2014) 16

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC)[1] is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts concerning privacy issues, new technologies, and constitutional interests: *See, e.g.*, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (No. 11-817); *United States v. Jones*, 132 S. Ct. 945 (2012); *Herring v. United States*, 555 U.S. 135 (2009); *Hiibel v. Sixth Judicial Dist. Ct. of Nevada, Humboldt County*, 542 U.S. 177 (2004); *State v. Earls*, 214 N.J. 564 (2013); *Commonwealth v. Connolly*, 454 Mass. 808 (2009).

EPIC has an interest in upholding Fourth Amendment protections against unreasonable searches and seizures. In particular, EPIC is focused on preventing the erosion of constitutional privacy rights due to the emergence of new technologies. Cell phone privacy is of critical concern to all Americans,

---

[1] Both parties have filed letters of consent consent to the filing of all amicus briefs with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

as sensitive private data is now routinely stored and accessed via Internet-enabled smartphones.

Technical Experts and Legal Scholars

James Bamford, Author and Journalist

Colin J. Bennett, Professor, University of Victoria

Christine L. Borgman, Professor & Presidential Chair in Information Studies, UCLA

Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law

Simon Davies, Project Director, London School of Economics

Laura K. Donohue, Professor of Law, Director of The Center for National Security and the Law, Georgetown University Law Center

David Farber, Distinguished Career Professor of Computer Science and Public Policy, School of Computer Science, Carnegie Mellon University

Dr. Addison Fischer, Former Owner, RSA Data Security, Co-Founder, Verisign

Hon. David H. Flaherty, Professor Emeritus of History and Law, University of Western Ontario; Information Privacy Commissioner for British Columbia, 1993-99

Deborah Hurley, Chair, EPIC Board of Directors

Jerry Kang, Professor of Law, UCLA School of Law

Chris Larsen, CEO, Ripple Labs Inc.

Harry Lewis, Gordon McKay Professor of Computer Science, School of Engineering and Applied Science, Harvard University

Anna Lysyanskaya, Professor of Computer Science, Brown University

Alice E. Marwick, Ph.D., Assistant Professor, Department of Communication and Media Studies, Fordham University

Mary Minow, Library Law Consultant

Dr. Pablo Molina, Adjunct Professor, Georgetown University

Dr. Peter G. Neumann, SRI International

Ray Ozzie, (former) Chief Software Architect, Microsoft

Dr. Deborah Peel, M.D., Founder and Chair, Patient Privacy Rights

Chip Pitts, Lecturer, Stanford Law School and Oxford University

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Eugene H. Spafford, Ph.D., D. SC., Professor, Purdue University

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Modern cell phone technology provides access to an extraordinary amount of personal data. Cell phone users routinely store sensitive and intimate information on a device that they keep close to their body. Misplacing a cellphone is an immediate cause for concern. Allowing police officers to search a

person's cell phone without a warrant following an arrest would be a substantial infringement on privacy, is unnecessary, and unreasonable under the Fourth Amendment. First, the warrantless search of a cell phone provides access to personal information and private files, stored both on the phone and on remote servers that are accessible from the phone. Second, there is no need to allow warrantless searches when currently available techniques allow law enforcement to secure the cell phone data pending a judicial determination of probable cause. Neither of the interests recognized by this Court underlying the search incident to arrest exception would justify the warrantless search of an individual's cell phone.

ARGUMENT

This case involves the warrantless search of Defendant's cell phone subsequent to his arrest. As this Court has repeatedly emphasized, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). This rule is subject to a few narrow exceptions, including certain searches incident to a lawful arrest. *Id.* However, no such exception justifies searching the vast array of information accessible from a cell phone without first establishing probable cause.

The search incident to arrest exception, outlined by the Court in *Chimel v. California*, 395 U.S. 752 (1969), and *United States v. Robinson*, 414

U.S. 218 (1973), is grounded in two interests: (1) the need to ensure officer safety and (2) the need to prevent the destruction of evidence. *Chimel*, 395 U.S. at 762-63. Searching a cell phone following an arrest serves neither of those interests.

In fact, modern cell phones provide access to so much information that a warrantless search would give the police unbridled access to that person's most sensitive information. Not only is the information on the device personal, users typically store account names, passwords, and other links to private data stored on remote computers. From a cellphone, users can even see into their homes and control devices and appliances.

Furthermore, the state's interest in obtaining evidence from the cell phone can be preserved without sacrificing Constitutional safeguards with simple and inexpensive security techniques. Best practices already recommend storing confiscated phones in packages, referred to as "Faraday bags," that block radio signals to prevent remote tampering. These simple and inexpensive procedures should be used to protect the phone and would give officers opportunity to obtain a judicial warrant to search the device if necessary.

The Fourth Amendment requires that officers obtain a warrant prior to conducting a search absent exigent circumstances. No special circumstances justify an exception to cell phones confiscated during a lawful arrest.

I. U.S. Consumers Are Dependent on Modern Cell Phones for a Wide Range of Personal and Business Activity

Cell phones are ubiquitous in the United States. More than 91% of American adults own a cell phone, Maeve Duggan, *Cell Phone Activities 2013*, PewResearch Internet Project (Sept. 19, 2013),[2] and wireless penetration – the number of active units divided by the total population – is over 100%. Fed. Commc'ns. Comm'n, *Mobile Wireless Competition Report (16th Annual)* 10 (Mar. 21, 2013).[3] The majority of phones are now sophisticated portable computers that provide constant Internet connectivity and a single point of access to all of the user's personal files, communications, and records. Phones are even expanding in size and functionality, and are now nearly equivalent to tablet computers. *See* Molly Wood, *Phone, Meet the Tablet.*, N.Y. Times, Feb. 27, 2014, at B8.

Cell phones are no longer simple communications devices used to send and receive calls, untethered from a wire. A majority of Americans now use Internet-enabled "smartphones" to send messages, surf the web, share photos, exchange files, get directions, use apps, and listen to music.[4] According to a recent poll, "Fully 68% of

---

[2] http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.

[3] *Available at* http://www.fcc.gov/reports/mobile-wireless-competition-report-16th-annual.

[4] According to AT&T, a smartphone is:

adults connect to the internet with mobile devices like smartphones and tablet computers." Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.*, PewResearch Internet Project (Feb. 27, 2014).[5]

Cell phones are also an increasingly important part of Americans' daily lives. As of June 2013, 56% of American adults use a smartphone. Aaron Smith, *Smartphone Ownership 2013*, PewResearch Internet Project (June 5, 2013).[6] Americans no longer use their phones solely for calling each other but also to browse online. PewResearch found that 63% of adult cell phone users use their phones to go online and

---

> a general term that refers to a cellular telephone that is more advanced than a feature phone. In general, a smartphone has an operating system that allows a user to do many of the things that were once reserved for a personal computer such as accessing the Web at higher speeds, viewing/editing documents, downloading files, creating music playlists, or managing multiple email/messaging accounts. Smartphones have advanced functionality, in addition to the standard functionality offered on a feature phone, such as the ability to send and receive text messages.

AT&T, *What is a Smartphone?* (2014), http://www.att.com/esupport/article.jsp?sid=KB101001&cv=821#fbid=m31wBrRSjwr.

[5] http://www.pewinternet.org/2014/02/27/summary-of-findings-3/.

[6] http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/

34% of these users go online mostly using their phones. *Id.* Americans use cell phones to send text messages (81%), access the Internet (60%), send or receive email (52%), download applications (50%), to get directions or location-based information (49%), to listen to music (48%), or to participate in a video call or video chat (21%). Maeve Duggan, *Cell Phone Activities 2013*, PewResearch Internet Project (Sept. 19, 2013).[7]

According to one industry report, 2013 was the first year that more than half of consumers (54%) no longer access the Internet from a single device (a desktop computer or a phone). The majority of Americans are now "multi-platform" users, meaning they browse the Internet from a combination of phones, computers, tablets, and other devices. This transition has been driven by the rising use of mobile applications ("apps"), with more than 85% of overall time on mobile phones spent within apps. Eli Goodman, *The Multi-Platform Majority: How Mobile is Changing the Way We Experience the Web*, comScore Blog (Dec. 9, 2013).[8] Mobile phones are already recognized as important tools with a wide range of educational, professional, and social uses. *See* Aaron Smith, *The Best (and Worst) of Mobile*

---

[7] http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.

[8] http://www.comscore.com/Insights/Blog/The_Multi-Platform_Majority_How_Mobile_is_Changing_the_Way_We_Experience_the_Web.

Connectivity, PewResearch Internet Project (Nov. 30, 2013).[9]

Consumers now use many different mobile apps on their cell phones to access personal data. The average smartphone user in 2013 had thirty-three mobile apps installed, and "actively" used twelve different apps during each thirty-day period. ThinkInsights, *Our Mobile Planet*.[10] A full 75% of smartphone users access the Internet via apps every day. *Id.*[11] Consumers prefer to access the Internet via apps, which account for "4 out of every 5 mobile minutes, rather than the mobile web." ComScore, *2013 Mobile Future in Focus* (Feb. 22, 2013).[12]

The market for applications is accelerating, according to *The Growing App Market* (2012).[13] The study notes that 47% of the U.S. population has downloaded at least one app, 24% have paid for an app and that among users with phones that can

---

[9] http://www.pewinternet.org/2012/11/30/the-best-and-worst-of-mobile-connectivity/.

[10] Graphs available for the United States and other countries at http://think.withgoogle.com/mobileplanet/en/. See relevant data under "Key Activities" -> "Apps" -> "Number of Apps on Smartphone."

[11] See relevant data under "Mobile Internet Usage" -> "Frequency Mobile Internet Usage via Apps" -> "Daily."

[12] *Available at* http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Mobile_Future_in_Focus

[13] *Available at* http://appdevelopersalliance.org/files/pages/The%20Growing%20App%20Market%20Slides%209-17-2012.pdf.

utilize apps, a full 74% of those users have downloaded an app. These apps enable cell phone users to access a variety of sensitive personal information stored either on the phone or remote Internet servers easily and seamlessly at any time.

In brief, the modern cell phone provides access to the single greatest concentration of personal information that could be conceived. For many users, their entire lives are accessible from their phones.

II. Modern Communications Providers Store Sensitive Personal Information on Remote Servers, Accessible to Authorized Users with Cell Phones, Tablets, and Other Devices

A majority of cell phone users now own smartphones, equipped with mobile applications that connect, synchronize, and deliver data stored and processed on remote servers. Many of these mobile "apps" allow users to access content across multiple platforms – on their phones, computers, and tablets. Modern phones not only provide access to files, messages, photos, and music, they also act as the keys that unlock a users' online identities. These devices provide access to remote repositories that contain private financial, medical, and communications records.

A. Mobile Apps Integrate Local and Remote Data to Provide Users With Access to Their Files and Communications

The proliferation of Internet-enabled mobile phones has fueled the development of mobile apps. *See* Pei Zheng & Lionel Ni, *Smart Phones and Next*

Generation Mobile Computing 51 (2010). These programs, downloaded and installed on the cell phone, access, display, and synchronize content that is stored remotely. The new generation of mobile apps download so much data that smartphone adoption has caused a "bandwidth jam in the United States," and mobile companies such as AT&T and Verizon are lobbying for additional wireless spectrum to increase capacity. *Communication Technology Update and Fundamentals* 260 (August E. Grant & Jennifer H. Meadows eds., 2012).

Users access e-mail messages, calendars, photographs, files, notes, and other personal data on all their devices – phones, computers, and tablets – via mobile apps. For example, Apple's service:

> iCloud stores your music, photos, apps, mail contacts, calendars, documents, and more and wirelessly pushes them to all your devices. So if you buy a song, take a photo, or edit a calendar event on your iPad, iCloud makes sure it appears on your Mac, iPhone, and iTouch, too.

Apple, *What is iOS 7* (2014).[14] *See also* Zheng & Ni, *supra* at 52 ("*E-mail, calendar, organizer, and notepad* are typical PIM [personal information manager] applications. Web-based PIM services such as Yahoo! allow users to synchronize personal data, including e-mail, personal calendars, organizers, and address books, from the web to PDA's or cell phones")

---

[14] http://www.apple.com/ios/what-is/.

(emphasis added). The e-mail apps on Apple iOS[15] and Android,[16] the two most common mobile operating systems, are configured to download new messages whenever the user opens the app. Many users configure their phones to receive e-mail messages automatically whenever they are available. *See* Rob LeFebvre, *Fetch or Push? Set Your E-mail Accounts to Maximize Battery Life, Speed of Delivery*, Cult of Mac (Aug. 5, 2013).[17]

Many mobile apps display a mix of locally stored and remotely synchronized content on the user's device. When a user opens an app, "Content such as pictures or video is [downloaded] over the Internet via a mobile data connection ([or] Wi-Fi), and once the content is embedded in the device (your smartphone), the data connection can be closed and the content viewed offline (when you aren't connected to the Internet." Peggy Anne Salz & Jennifer Moranz, *The Everything Guide to Mobile Apps* 15 (2013).

These programs, widely used on cell phones today, rely on remote servers that continuously

---

[15] *See* Apple, *iPhone User Guide* 49 (2013), *available at* http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

[16] *See* Google, *Android Quick Start Guide* 36 (2013), *available at* http://static.googleusercontent.com/media/www.google.com/en/us/help/hc/images/android/android_ug_42/Android-Quick-Start-Guide.pdf.

[17] http://www.cultofmac.com/238746/fetch-or-push-set-your-email-accounts-to-maximize-battery-life-speed-of-delivery-ios-tips/.

transfer data back and forth between the devices and the servers. This model of computing is sometimes described as "cloud computing."[18] When a user views or searches their e-mail, photographs, financial records, or other sensitive information from a mobile apps, that data is downloaded from the server to the phone as it is presented to the user alongside previously downloaded data.

From the user's perspective, the data that is stored on the phone and the data that is stored in the cloud and available on the phone are often indistinguishable. App data is continuously updated in order to ensure that the data is synchronized across all the users' devices. According to Deloitte, the rise in "converged, connected devices" leads to a situation where "consumers are increasingly storing and synchronizing files in the cloud," such that by the end of 2013, "there will be some 600 million personal cloud subscriptions, and that number is expected to double by the end of 2017." Deloitte, *The State of the Global Mobile Consumer* 6 (2013).[19] In fact, many apps now provide updates even when the user does not have them open. *See* Apple, *iOS: Understanding Notifications* (2014).[20] By default, Apple devices allow

---

[18] For a brief description of cloud services, see Goodwill Community Foundation, *What is the Cloud?* (2014), http://www.gcflearnfree.org/computerbasics/extra/82.

[19] *Available at* https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT-GMCS_January%202014.pdf.

[20] http://support.apple.com/kb/ht3576.

these notifications to be viewed even when the phone is locked. *Id.*

This cloud-based model attempts to ensure that the user will see the same messages, files, and records no matter where they are. The data "stored" on the phone might provide a momentary snapshot of the user's activities, but the phone will continue to download additional data from remote servers. Modern phones are constantly downloading, or "pulling" new data and remote servers are constantly sending, or "pushing," updates, including private messages, breaking news, and alerts.

B. Mobile Apps Provide Access to Sensitive Information on Remote Servers

The popularity of smartphones has lead to an explosion in mobile apps. For users of just one popular cell phone, there are now more than 1 million different apps available. *See* Chuck Jones, *Apple's App Store to Hit 1 Million Apps*, Forbes (Dec. 11, 2013);[21] AppBrain, *Number of Available Android Apps in the Market* (2014).[22] These programs enable users to access a variety of services and download up-

---

[21] *Available at* http://www.forbes.com/sites/chuckjones/2013/12/11/apples-app-store-about-to-hit-1-million-apps/. According to a popular Apple iOS development page, there are 1,135,438 active apps in the Apple store. *Apple Store Metrics*, http://148apps.biz/app-store-metrics/ (last visited Mar. 7, 2014).

[22] http://www.appbrain.com/stats/number-of-android-apps. There were 1,132,053 available Android apps as of February 13, 2014. *Id.*

to-date information. Many of these apps connect users with sensitive personal data that is stored on remote servers, including:

- E-mails and messages
- Calendars
- Notes
- Personal files
- Financial records, and
- Medical records

Some apps enable direct remote control of systems and devices within the users' homes.

Messaging Services

Mobile phone users rely on a variety of applications to send electronic communications. Email providers such as Google store older emails in the cloud. Google, *Gmail Help: Open & Read Email* (2014).[23] These messages can then be accessed by the user (or anyone in possession of the phone), by either scrolling down or conducting a keyword search. *Id.* The email provider then pulls the relevant messages

---

[23]https://support.google.com/mail/topic/2819493?hl=en&ref_topic=2772286. *See also* Google, *Getting Started with IMAP and POP3* (2014), https://support.google.com/mail/troubleshooter/1668960?hl=en (Google "encourage[s] you to use IMAP" because "IMAP offers two-way communication between your web Gmail and your email client. This means when you log into Gmail using a web browser, actions you perform on email clients and mobile devices . . . will instantly and automatically appear in Gmail").

from the cloud and makes them visible to the mobile phone user. *Id.*

Mobile phones also provide access to online social networking tools. Online social networking tools contain a variety of sensitive personal information, including information about users' associations and friendships, photographs, and communications.

Most social networks provide private messaging services in addition to public message posting. Facebook, the most popular social network service, with over 1.23 billion users worldwide and 945 million monthly mobile users, Facebook, *Key Facts* (2014),[24] allows users to add friends, communicate privately via either an instant messaging tool, an email-like messaging service, or both. Twitter, another popular social network, has over 645 million users, 43% of which use their phone to tweet. Statistic Brain, *Twitter Statistics* (Jan. 1, 2014).[25] Twitter users can publicly post text or picture messages – "tweets" – or can send private, "direct messages" to other users.

As of October 2013, Google's social network, Google+ had 540 million active users, including 300 million monthly users, who uploaded an average of 1.5 billion photos every week. Matt McGee, *Google+ Hits 300 Million Active Monthly "In-Stream" Users, 540 Million Across Google*, Marketing Land (Oct. 29,

---

[24] http://newsroom.fb.com/Key-Facts.

[25] http://www.statisticbrain.com/twitter-statistics/.

2013).[26] Google+ also allows users to make public posts, limited-audience posts, and to send private communications to other users.

These social networks are easily accessible on cell phones with mobile apps. These apps provide access to a user's account, including private communications, personal photographs, and contact lists. Facebook, Twitter, Google+ and Snapchat all have popular mobile apps. In fact, according to Adobe's 2013 Mobile Consumer Survey, accessing social media is "the number one mobile activity today. . . .Of those surveyed, 71% reported using their mobile device to access social media." Ray Pun, *Adobe 2013 Mobile Consumer Survey: 71% of People Use Mobile to Access Social Media*, Adobe Digital Marketing Blog (July 25, 2013).[27]

Photo and Video Sharing

Mobile phone applications also allow users to access and share photographs and videos. YouTube enables cell phone users to send private videos to other cell phone users. YouTube, *Video Privacy Settings* (2014).[28] These videos can include very personal user-created content. YouTube's application allows a user to access his or her playlists of videos,

---

[26] http://marketingland.com/google-hits-300-million-active-monthly-in-stream-users-540-million-across-google-63354.

[27] http://blogs.adobe.com/digitalmarketing/mobile/adobe-2013-mobile-consumer-survey-71-of-people-use-mobile-to-access-social-media/.

[28]https://support.google.com/youtube/answer/157177?hl=en

which are stored on the company's external servers. Google Play Store, *YouTube Application Page* (2014).[29]

Flickr is a photo hosting service that has similar features. The service allows users to upload photographs, which may be shared publicly or kept private. Yahoo!, *Privacy Policy: Flickr* (2014).[30] Users can "choose to make your photos default to public for anyone to access, restrict access to a limited number of other Flickr users, or keep those photos private so only you can access them." Like YouTube, Flickr has a mobile application that allows the user to access remotely stored photos, including photographs that have been designated as "private," on a mobile device. Google Play Store, *Flickr Application Page* (2014).[31]

Apple also has a built-in photo-sharing feature for iPhone users. *See* Apple, *iCloud Photo Sharing* (2014).[32] This app allows users to create and share photos with other users, and "each new addition is instantly broadcast to the photo stream of everyone in your group." *Id.* Users even get "real time notifications" of updates or new photos posted to their streams. *Id.* This means that at any time a users

---

[29]https://play.google.com/store/apps/details?id=com.google.android.youtube&hl=en.

[30] https://info.yahoo.com/privacy/us/yahoo/flickr/details.html.

[31] https://play.google.com/store/apps/details?id=com.yahoo.mobile.client.android.flickr.

[32] https://www.apple.com/icloud/icloud-photo-sharing.html.

phone could automatically receive new private photos from their friends, without even opening the app.

Personal Information Managers

There are many services, operating on cell phones, designed to assist in the management of personal information. For example, Evernote, promises, "all of your notes, web clips, files, and images are made available on every device and computer you use." Evernote, *Keep Everything in Sync* (2014).[33] Google provides a similar service with Google Sync, which encourages users to "Sync your Google services to your phone, tablet, and desktop programs, so that you can always access what's important to you." *See* Google, *Sync Your Mail, Contacts, Calendar, and More* (2014).[34] Other services enable businesses to managing their schedules and information remotely. For example, Full Slate includes an online scheduler, Calendar Sync, an appointment app for iPhone or Android, and a Client Database to "keep track of contact information, appointment history, and email correspondence in one place." Full Slate, *Client Database* (2013).[35]

All of these services enable access to detailed personal information directly from a cell phone.

---

[33] http://evernote.com/evernote/.

[34] http://www.google.com/sync/.

[35] https://www.fullslate.com/client-database.

Remote File Storage

File storage is one of the most popular cloud-based services. These services allow users to store, access, edit, and share their files, including word processing documents, presentations, spreadsheets, pictures, music, and videos. Some of the most popular file-storage services are Dropbox,[36] Apple's iCloud,[37] Amazon Cloud Drive,[38] Box,[39] Google Drive,[40] MediaFire,[41] and Windows Live OneDrive.[42]

Many of these file storage services can be accessed from mobile apps installed on a cell phone, allowing the user to access the information, even though the information is not itself stored on the phone. These files are private and can include a great deal of sensitive personal information – financial records, private messages, photographs, personal notes, and health records.

A person in possession of the cell phone therefore has access to this information even though it is stored on remote servers.

---

[36] *Dropbox*, https://www.dropbox.com/ (2014).

[37] *Apple iCloud*, https://www.apple.com/icloud/ (2014).

[38] Amazon, *Cloud Drive Photos for iOS* (2014), https://www.amazon.com/gp/feature.html/ref=cd_nav_ios?ie=UTF8&docId=1001206201.

[39] *Box*, https://www.box.com/ (2014).

[40] *Google Drive*, https://drive.google.com (2014).

[41] *Media Fire*, http://www.mediafire.com/ (2014).

[42] *Windows Live OneDrive*, https://onedrive.live.com/about/en-us/ (2014).

Financial Records

The entire world of personal finance is moving on to the cell phone. Mobile banking is "on the cusp of transformation from a niche service for the technologically elite to a mass-market service demanded by all customer segments." Deloitte Consulting, *Mobile Banking: A Catalyst for Improving Bank Performance* (2010).[43] At the time Deloitte noted that 10% of mobile users conduct some banking transactions via phone and that mobile banking usage increased at "nearly a 100% compounded annual growth rate" from 2005-2010, with most of the growth concentrated after 2007. *Id.*

The Federal Reserve recently described mobile banking as "using a mobile phone to access your bank account, credit card account, or other financial account. Mobile banking can be done either by accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone." Bd. of Gov's of the Fed. Reserve Sys., *Consumer and Mobile Financial Services 2013* (Mar. 2013).[44]

---

[43] *Available at* https://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_consulting_MobileBanking_010711.pdf.

[44] *Available at* http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf (last visited Feb. 28, 2014).

According to the Federal Reserve, in 2013, 28% of all mobile phone users and 48% of smartphone users, have used mobile banking within the past twelve months. The most common use of mobile banking is to check account balances or recent transactions (87%). 15% of mobile phone users have made a mobile payment within the past twelve months, *Consumer and Mobile Financial Services 2013*, *supra* at 4, and 49% of mobile banking users utilize mobile apps to conduct their mobile banking transactions. *Id.* at 10.

The main reason more consumers do not use mobile banking is concern about security (38%). *Id.* at 14. The sensitivity of financial information underscores the privacy concerns that arise when this data is accessible from a phone.

Mobile apps also provide access to other financial data. For example, Mint is a popular financial tracking app that aggregates all of a user's financial accounts and records into one place. *What is Mint* (2014),[45] Many banks also have dedicated apps that provide their customers with mobile account access. *See, e.g.*, Bank of America, *Mobile Banking* (2014);[46] Wells Fargo, *Mobile App* (2014);[47] Chase, *Mobile App* (2013).[48] Thus, a user's current financial

---

[45] https://www.mint.com/what-is-mint/.

[46] https://www.bankofamerica.com/online-banking/mobile.go.

[47] https://www.wellsfargo.com/mobile/apps/.

[48] https://www.chase.com/content/chasecom/en/mobile-banking/mobileresponsive.

statements, stored on the bank's remote server, are easily accessible via an app on their phone.

Medical Records

Many users rely on their cell phones to access sensitive medical information, including records detailing medical conditions, exercise, nutrition, menstrual cycles, and medication use. According to Pew Research, 19% of smartphone users have a health app on their phone. Susannah Fox and Maeve Duggan, *Mobile Health 2012*, PewResearch Internet Project (Nov. 8, 2012).[49]

Some of these applications provide complete access to medical history files that would disclose sensitive information about health conditions and medications. The Medicare Blue Button allows patients to download their medical history into a simple text file on their smartphone. Elizabeth Stawicki, *Your Smartphone Might Hold Key to Your Medical Records*, Kaiser Health News (June 17, 2013).[50] Third party applications then help the user organize this information. Cloud-based document storage system Box provides a medical record storage system called "drchrono" that "is a medical platform for doctors and patients. The platform is divided into cloud based electronic health records, practice management, personal health records, and revenue

---

[49] http://www.pewinternet.org/2012/11/08/mobile-health-2012/.

[50] http://www.kaiserhealthnews.org/stories/2013/june/17/electronic-health-records-blue-button.aspx.

cycle management. The primary purpose of drchrono is to provide mobile healthcare through iPad, iPod touch, and iPhone." Box, *drchrono Description* (2014).[51]

Other applications allow users to log information about their fitness habits, *The Fitbit Story* (2014),[52] nutritional intake, *id.* ("Log your food with Fitbit's online tools and mobile apps to get a more complete view of your health and fitness."), menstrual cycles,[53] blood pressure,[54] and medication times.[55]

As with financial information accessible from a cell phone, users have expressed a clear desire for privacy regarding health data. Deloitte Consulting reports that 35% of survey respondents stated that they were concerned that the privacy and security of

---

[51] https://app.box.com/services/drchrono (last visited Feb. 28, 2014).

[52] http://www.fitbit.com/story ("Track everyday activity like steps, distance, calories, stairs climbed, and active minutes").

[53] Tamtris Web Services Inc., *Fertility Friend*, iTunes Preview (2014), https://itunes.apple.com/us/app/fertility-friend-ovulation/id443919067?mt=8.

[54] Taconic System LLC, *Blood Pressure Monitor*, iTunes Preview (2014), https://itunes.apple.com/us/app/blood-pressure-monitor-family/id430133691?mt=8.

[55] Medisafe Project, MediSafe Meds & Pill Reminder, Google Play Store (2014), https://play.google.com/store/apps/details?id=com.medisafe.android.client.

their personal information might be at risk when using a mobile device to access health records or tests online. Deloitte Consulting, *mHealth: a Check-up on Consumer Use* (2014).[56]

Remote Desktop Clients

Mobile apps even enable users to access their home computers remotely from their cell phone. From these "remote desktop" apps, users can view and control their desktop computers, including running programs, viewing files, and connecting to the remote network. *See* Citrix, *GoToMyPC: Remote Access Factsheet* (2013).[57]

This means that if a user has installed the software on their home or work computer, and configured the mobile app on their cell phone, anyone with access to the phone can "simply open the app," enter the user's credentials, and be "instantly connected to" that remote computer. Citrix, *GoToMyPC: Total Mobility – Factsheet* (2013).[58] These apps are especially popular with employers now because they can be used to "[i]ncrease employee productivity and flexibility." *Id.*

---

[56]http://www.deloitte.com/view/en_US/us/Insights/centers/center-for-health-solutions/5aa32defd7b21410VgnVCM2000003356f70aRCRD.htm.

[57] *Available at* http://l1.osdimg.com/remote-access/dam/pdf/white-papers/GoToMyPC_Factsheet.pdf.

[58] http://l1.osdimg.com/remote-access/dam/pdf/white-papers/GoToMyPC-Mobile-Remote-Access-Factsheet.pdf.

As a consequence, possession of a cell phone may provide access not only to files maintained by third party companies on the user's behalf but also to personal information stored directly on computers within the user's home.

Internet-enabled Home Appliances

Mobile phones now also provide for direct control of appliances and utilities in the user's home. Ninety-three percent of smartphone users recently expressed interest in using their mobile phones to remotely control their home temperature, lights, and other utilities. Wi-Fi Alliance, *Connect Your Life: Wi-Fi and the Internet of Everything* 9 (2014).[59]

For example, General Electric offers the GE Brillion App to control home appliances, such as ovens via your smartphone. General Electric, *GE Brillion Connected Appliances* (2014).[60] Currently, the GE Brillion App only works with GE Double Wall or Single Wall Ovens, but GE notes that "Coming in 2014, GE will expand its line of Brillion-enabled appliances." *Id.* Nest, recently acquired by Google, has devised the Nest Thermostat, which "can learn your schedule, programs itself, and can be controlled from your phone." Nest, *Life with Nest Thermostat* (2014).[61] Nest also makes a smoke alarm that can

---

[59] *Available at* http://www.wi-fi.org/system/files/wp_Wi-Fi_Internet_of_Things_Vision_20140110.pdf.

[60] http://www.geappliances.com/connected-home-smart-appliances/.

[61] https://nest.com/thermostat/life-with-nest-thermostat/.

send mobile alerts to your phone when an alarm sounds and whose features can be controlled from the mobile application. Nest, *Smoke Co-Alarm, Inside & Out* (2014).[62]

The Nest App, installed on a cell phone, can control both the Nest Thermostat and Smoke Alarm, which enables you to "change the current target temperature or view your energy usage on your Nest Thermostat, view the latest status, and adjust the settings on your Nest Protect, and much more." Nest, *Learn More about the Nest App* (2014).[63]

These mobile applications provide access to the inside of a home even when outside the home. The apps also give police officers who seize a cell phone access to data about the inside of the home and the possibility of affecting the internal temperature, turning on or off the gas furnace, and detecting historical variations in temperature. They provide information regarding the homeowner's schedule ("To save energy, Nest learns your schedule and preferences to program itself." Nest, *Saving Energy* (2014).[64] Possession of the cell phone could therefore provide intimate information to police about the activities of an individual within their home, without police ever obtaining a warrant to search the home.

---

[62] https://nest.com/smoke-co-alarm/inside-and-out/#teardown.

[63] http://support.nest.com/article/Learn-more-about-the-Nest-app.

[64] https://nest.com/thermostat/saving-energy/#we-didnt-think-thermostats-mattered-either.

C. Cell phones also operate much like a password, providing access to remote files and information that would not be available to an unauthenticated user

Mobile apps provide users with access to a wealth of private data, but they also provide an easy way to access and consolidate user's various online identities – social media accounts, bank accounts, e-mail accounts, and other profiles. Users are typically required to create unique, complex passwords for their various accounts. This can be a headache for many users. *See* Troy Hunt, *The Only Secure Password is the One You Can't Remember*, Lifehacker (Mar. 24, 2011);[65] Phillip Inglesant & M. Angela Sassse, *The True Cost of Unusable Password Polices: Password Use in the Wild*, Proc. SIGCHI Conf. Hum. Factors Comp. Sys. (2010) ("We find that users are in general concerned to maintain security, but that existing security policies are too inflexible to match their capabilities, and the tasks and contexts in which they operate.").[66]

But most mobile devices now solve this problem by storing passwords and other login information on the device so that the person in possession of the device is able to access all of the password-protected services. Apple now offers a similar service as part of its iPhone software. *See*

---

[65] http://lifehacker.com/5785420/the-only-secure-password-is-the-one-you-cant-remember.

[66] *Available at* http://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf.

Apple, *What is iOS* (2014) ("Most websites you visit nowadays require user names and passwords. Remembering them all can be tough. So let iCloud Keychain do it for you."). Some mobile apps also keep users logged in by default. Other apps provide storage of user login information for many sites and applications in one place. This means that a user's online identities are all easily accessible to anyone who has access to their phone.

Many applications have password saving features and generally, "by default, applications will store your passwords and never ask you for them again." Jonathan Garro, *Mac Computer Skills: Unlock the Power of Your Mac's Keychain Utility*, Tuts+ (April 15, 2013).[67] For example, when a user logs into Facebook via their cell phone, the app will keep the user logged in by default and store the password information. Some social media accounts, such as Twitter and Facebook, are even embedded into the phone software, requiring the user to take affirmative steps to log out. *See* Twitter, *How to Sign Out of Twitter for iPhone* (2014);[68] Facebook, *How do I log out of the iPhone or iPad App?* (2014).[69] This is a desired feature for many mobile phone users due to

---

[67] http://computers.tutsplus.com/tutorials/unlock-the-power-of-your-macs-keychain-utility--mac-48730.

[68] https://support.twitter.com/groups/54-mobile-apps/topics/222-ios/articles/20170805-how-to-sign-out-of-twitter-for-iphone#.

[69] https://www.facebook.com/help/iphone-app/112099682212213?rdrhc.

its convenience and is widely utilized. But it poses a serious privacy problem if law enforcement officers are allowed to access the user's phone without probable cause.

Users can also install a specific app, called a password manager, to store all of their online login information. Many of these password managers are available for current smartphones, including Last Pass, Onesafe, and 1Password. Kit Eaton, *Apps to Protect Your Array of Passwords,* N.Y. Times, Oct. 17, 2013, at B10. The user enters the passwords for all the websites and applications they wish to use, including banking, medical, and other extremely sensitive accounts they may have. These passwords are secured by a master password. The password manager then logs into the various other applications without the user needing to enter log in information. As with the in app storage of passwords, the data stored on the phone provides access to large amounts of data not stored on the phone.

In addition to storing passwords that provide access to a user's online identities, the smartphone can also be used to authenticate the user on other systems. This type of authentication, commonly referred to as "two-factor authentication," is offered by companies such as RSA (RSA SecureID Software Authenticators)[70] and Google (Google

---

[70] RSA, *RSA SecurID Authenticators: The Gold Standard in Two Factor Authentication* (2011). Available at: http://www.emc.com/collateral/data-sheet/h9061-sid-ds.pdf.

Authenticator).[71] Two-factor authentication requires that a user enter a unique numeric code, generated by a phone or other device, in addition their password to access the account. This prevents an unauthorized individual from accessing an account simply by knowing the password. In this way, cell phones act as a "key" to the user's online and offline identities.

Thus, a mobile phone acts as a master key that can grant access to, and prove a connection with, all of the user's various online and offline identities. The phone provides a portal to personal data stored on the cloud. Like a password, control over the phone is control over the data.

New apps can even replace physical keys and provide entry into a user's automobile or home. Bluetooth technology works with all vehicles and all Bluetooth enabled cell-phones, from a range of 5-15 feet, to unlock the user's car without a key. The product is designed so that "you can simply approach the vehicle which will unlock automatically. As you leave the parked vehicle, the module will also lock the vehicle." Bluetooth Keyless, *FAQs About the Bluetooth Passive Keyless Entry Module* (2014).[72] For customers who buy the Premium version of the product, the company provides an app customized to the individual phone's operating system such as iOS or Android. *Id.* An officer armed with this app could

---

[71] Google, *Google Authenticator* (2014), https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2.

[72] http://bluetoothkeyless.info/bluetooth-keyless-information/.

identify the user's car and even unlock it from nearby. Similar functionality exists for home entry. Lockitron, *Keyless Entry Using Your Phone* (2014).[73]

III. Law Enforcement Can Easily Mitigate the Risk of Cell Phone Data Loss Pending a Judicial Determination of Probable Cause

Cell phones may contain data, such as location data, text messages, and pictures, that may be useful as evidence to law enforcement,. Rizwan Ahmed, Dr. Rajiv V. Dharaskar, & Dr. Vilas M. Thakare, *Digital Evidence Extraction and Documentation From Mobile Devices*, 2 Int'l J. Advanced Res. Comp. & Comm'n Eng. 1019, 1022 (Jan. 2013). This data is stored in either the subscriber identity module (SIM) card, which contains information necessary for identifying the device on the cell network, Eoghan Casey & Benjamin Turnbull, *Digital Evidence on Mobile Devices*, in *Digital Evidence and Computer Crime* 5 (2011),[74] other external memory, such as an SD card which can be easily removed from the device, *id.* at 6, and the internal memory, which cannot be easily removed from the device. *Id.*

The standard for mobile devices, including laptops and cells phones, is to utilize a type of storage called flash memory. *Id.* at 3. Flash memory is non-volatile, meaning that the data will be retained even

---

[73] https://lockitron.com/.

[74] *Available at* http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf.

if the storage device is powered down. Russell Kay, *Flash Memory*, ComputerWorld (June 7, 2010).[75] Because flash memory only has a limited number of times data can be written on it, deleted data can remain for some time. Casey & Turnbull, *supra* at 3. This depends on the methods used to delete the data. Thorough sanitization of flash-based storage requires writing over the data multiple times, which lowers the life expectancy of the hardware. *See* Michal Wei et al., *Reliably Erasing Data From Flash-Based Solid State Drives*, 9th USENIX Conf. File & Storage Tech. (2011).[76]

A. Standard, Low-cost Security Techniques Enable Law Enforcement to Significantly Reduce the Risk of Cell Phone Data Loss

Some courts have expressed concern that cell phone data could be "remotely wiped" subsequent to a user's arrest. *See United States v. Flores-Lopez*, 670 F.3d 803, 807-808 (7th Cir. 2012). However, this concern can be easily mitigated with currently available security measures, and does not justify the warrantless of a confiscated device. Once the phone is secured, law enforcement officers can obtain a

---

[75] http://www.computerworld.com/s/article/349425/Flash_Memory.

[76] https://www.usenix.org/conference/fast11/reliably-erasing-data-flash-based-solid-state-drives (last visited Mar. 10, 2014).

warrant based on probable cause to search the phone if necessary.

There are three techniques that can preserve data on cell phones while a warrant is obtained: the use of data extraction devices, Faraday Bags, and aluminum foil. There is also the simple step of removing the battery from the device

Current best practices recommend that law enforcement officers turn off cell phones immediately upon confiscation. For example, the Drug Enforcement Administration guidance to law enforcement departments warns that officers "should be aware that when seizing a cell phone, the owner can remotely delete all personal data from the phone." El Paso Intelligence Center, *Tactical Intelligence Bulletin EB 11-09: Preserving Cell Phone Data* (2011).[77] The DEA recommends that the battery be immediately removed so that remote wiping signals cannot be received and that if the battery cannot be removed, the cell phone should either 1) be wrapped in aluminum foil or 2) be placed in a Faraday type box, which prevents the signal from being received. *Id.*

The Association of Chief Police Officers ("ACPO") in the United Kingdom has created a similar practice guide for handling electronic evidence, which includes a section entitled "Guide for Mobile Phone Seizure & Examination." Association of

---

77

https://www.ileas.org/sites/default/files/Preserving%20cell%20phone%20data.pdf.

Chief Police Officers, *Good Practice Guide for Computer-based Electronic Evidence* 48 (2008).[78] The ACPO Principles of Evidence provide basic guidance for police officers seizing evidence from electronic media. *Id.* at 4.[79] This ACPO advises officers when seizing a device to "Isolate the device from the network" and suggests officers: "Turn Device off at point of seizure," or "Place Device in shielded container/bag." *Id.* at 48. When examining the mobile

---

[78]http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[79] The Principles state:

> Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
>
> Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
>
> Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

phone, the ACPO recommends that a shielded room or container be used, but discourages the use of jamming devices, which are often illegal. *Id.*

The National Institute of Standards and Technology ("NIST") addressed this issue in a report on Cell Phone Forensics. Nat'l Inst. of Stds & Tech, *Guidelines on Cell Phone Forensics*, Special Pub. No. 800-101 (May 2007).[80] In this report, NIST applied the ACPO Principles of Evidence and emphasizes the need to "isolate the phone from other devices used for data synchronization" and reaffirmed that the basic methods to isolate the phone from a radio network are to turn the device off or to place it in a shielded bag. *Id.* at 33-34. NIST also stated that putting the phone in "Airplane Mode" is another alternative, but has the drawback of "requiring interaction with the phone via the keypad, which poses some risk." *Id.* at 34.

Faraday Bags

To block the radio network signal, one commonly used tool is a Faraday bag. These are "specially designed RF [radio frequency] plastic coated shielded bags used to shield a mobile device from external contact. The bags are coupled with a conductive mesh to provide secure transportation to the laboratory." David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices For Use*

---

[80] *Available at* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

in Criminal Investigations, Forensic Focus, Aug. 20, 2011.[81] One potential disadvantage of the bag is that the phone can continue to search for a signal, potentially draining the battery while being transported to the laboratory. One possible solution is to hook the phone up to what is called a trickle charger, a small charging device that can be placed within the Faraday bag with the phone. Greg Gogolin, *Digital Forensics Explained* 59-60 (2013). It is also possible that the phone's location data can be overwritten during transport, but the Faraday bag will prevent a remote wiping command from being executed.

One company, Paraben, makes what it calls "Wireless Stronghold Bags 2.0," which it claims is more than 99.999% effective in blocking wireless signals across multiple frequencies. The basic Paraben cellphone bag is available for $39.95. Paraben, *Wireless Stronghold Bags 2.0* (2013).[82]

Aluminum Foil

The main component in a Faraday bag is aluminum foil and so the effect can be replicated simply through wrapping the phone in aluminum foil.

---

[81] *Available at* http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/.

[82] https://www.paraben.com/downloads/sh-bag-brochure.pdf.

The police officer can cover the phone in foil, thus preventing the cell phone from receiving a network signal and executing a remote wiping command. Eamon P. Doherty, *Digital Forensics for Handheld Devices* 14 (2013). The primary disadvantage with the aluminum foil is that its effectiveness has not been tested as fully as Faraday bags; Faraday bags are thus preferred over aluminum foil because the use of foil "could offer an unwanted line of questioning in court." *Id.*

Furthermore, when police have seized the phone and prevented it from receiving a network signal, there is a broad array of tools available to extract data. Modern Data Extraction Devices are capable of obtaining many types of information from personal electronic devices such as cellphones, tablets, and GPS. They can bypass lockscreen and password protections, and recover information that has been previously deleted. A company called Cellbrite makes a device called the Universal Forensics Extraction Device ("UFED") Touch Ultimate that is capable of recovering a wide variety of data files. The device can recover "existing and deleted data: apps, passwords, emails, call history, SMS, contacts, calendar, media files, geotags, location information, GPS fixes, etc." Cellbrite, *UFED TOUCH Ultimate: All-inclusive Mobile Forensic Solution* (2013).[83] The device is designed to be compatible with a wide range of phones on the

---

[83]http://www.cellebrite.com/images/stories/brochures/UFED-Touch-Ultimate-ENGLISH-web.pdf.

market, including Blackberry, IOS, Android phones, and Windows Phones. *Id.*

Pareben Corporation sells a produce called Device Seizure that is preferred by many forensic investigators "because it has some capability to collect information from cell phones, PDAs, and some GPS devices for use in the car. Companies that wish to save money often look for one product that can do more than one purpose..." Eamon P. Doherty, *Digital Forensics for Handheld Devices* 18 (2013).

B. Similar Security Procedures Have Already Been Adopted by Federal Agencies to Protect Sensitive Data in Other Contexts

The federal government has already adopted a number of security protocols to protect sensitive data, similar to the use of signal-blocking packages discussed above. It is clear from existing agency procedures that it would not be unreasonably burdensome to implement similar procedures to protect sensitive cell phone data pending a judicial determination on any warrant application.

In 2004, the State Department announced a plan to install Radio Frequency Identification ("RFID") chips in all newly issued passports. The RFID technology would allow State Department officials to obtain the passport holder's identifying information using radio waves read from a distance but would also allow others to access the content of the passport.

EPIC and other privacy experts and security researchers opposed this proposal, noting that this

technique would unnecessarily expose traveler's sensitive personal information to others, and that technical measures could be adopted to minimize the risk. *See See* Comments of Electronic Privacy Information Center to State Dep't, Dkt. No. DOS-2006-0329 (2007) (RFID tags "creates significant security and privacy risks, particularly if individuals are not able to control the disclosure of identifying information").[84] *See also* Bruce Schneier, Opinion, *Does Big Brother Want to Watch?: Passport Radio Chips Send Too Many Signals*, N.Y. Times, Oct., 4, 2004 ("Unfortunately, RFID chips can be read by any reader, not just the ones at passport control. The upshot off this is that travelers carrying around RFID passports are broadcasting their identity").[85]

Privacy groups argued that the use of contactless technology (where the passports could be read through the air rather than being swiped) left the passports vulnerable to surreptitious, unauthorized access from users who possessed compatible readers. Letter from Electronic Frontier Foundation, EPIC, Privacy Activism, Privacy Rights Clearinghouse, and World Privacy Forum to Legal Division Chief, Office of Passport Policy, Planning and Advisory Services, U.S. Dep't of State (April 4, 2005).[86] Furthermore, the RFID technology would

---

[84] *Available at* http://www.epic.org/privacy/us-visit/comm120605.pdf.

[85] *Available at* http://www.nytimes.com/2004/10/04/opinion/04iht-edschneier_ed3_.html.

allow unauthorized users to engage in clandestine tracking of the passport holder via the unique ID numbers attached to each RFID chip. *Id.* at 12. Finally, a lack of encryption left a host of valuable identity information, including biometric data, vulnerable to exfiltration. *Id.* at 13.

In response, the State Department adopted the recommendations of privacy and security experts, and amended the protocol to include an RFID-shielded sleeve in the passport, which prevents remote scanning when the passport is closed. U.S. Dep't of State, *Bureau of Consular Affairs*.[87] The State Department also encrypted the data on the chip and put the key for the encryption on the passport. The new process involved a contact technology whereby "a customs officer swipes the passport through the optical reader to get the key, and then the RFID reader uses the key to communicate with the RFID chip." Bruce Schneier, *Fatal Flaw Weakens RFID Passports*, Wired (Nov. 3, 2005).[88]

These changes to improve the security of the passport information demonstrate the capacity of the government to implement technological measures that protect sensitive personal data from wireless access. A Faraday bag would be a far less expensive technique for securing a seized cell phone than was

---

[87]http://travel.state.gov/content/passports/english/passports/information/card.html.

[88]http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69453?currentPage=all

the State Department's decision to redesign the passport to address concerns about remote access.

The government also has the capacity to protect sensitive information through the use of specially constructed rooms, built to high standards. These are called Sensitive Compartmented Information Facilities ("SCIFs") and are present throughout the government to protect information that has a high security requirement. Many government agencies utilize these facilities, both to store sensitive information and to create a space in which this information can be discussed. Adamo Construction, Inc., *What is a SCIF or Sensitive Compartmented Information Facility?* (2014).[89] SCIFs have substantial construction requirements, which are laid out in Intelligence Community Directive (ICD) 705/IC Technical Specification.[90] SCIFs can either be permanent structures or mobile and temporary depending on the needs of the user. In either case, the materials used in construction of the facility are chosen to prevent electronic signals from either entering or exiting the secured location. In the case of mobile SCIFs, such as the ones utilized by the President while overseas, a shielded tent provides sufficient protection from electronic surveillance.

---

[89] http://www.adamoconstruction.com/what-is-scif.php.

[90] Office of the National Counterintelligence Executive, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.2* (2012), *available at* http://www.fas.org/irp/dni/icd/ics-705-ts.pdf.

Rajini Vidyanathan, *Barack Obama's Top Secret Tent*, BBC News (March 22, 2011).[91]

Such methods demonstrate the ready availability of techniques that would allow the police to preserve evidence on a cell phone so that a warrant may be obtained prior to the search of a device containing, and providing access to, an extraordinary amount of detailed, personal information.

---

[91] http://www.bbc.co.uk/news/world-us-canada-12810675.

CONCLUSION

For the foregoing reasons, *amicus* respectfully ask this Court to reverse the decision of the California Court of Appeal below.

Respectfully submitted,

MARC ROTENBERG
GINGER MCCALL
ALAN BUTLER
DAVID HUSBAND
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

March 10, 2014

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

Nos. 13-132 & 13-212

IN THE
SUPREME COURT OF THE UNITED STATES

DAVID LEON RILEY,
Petitioner,
v.
STATE OF CALIFORNIA,
Respondent.

On Writ of Certiorari to the California Court of Appeals, Fourth District

UNITED STATES OF AMERICA,
Petitioner,
v.
BRIMA WURIE,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the First Circuit

BRIEF OF *AMICI CURIAE* – PROFESSORS CHARLES E. MACLEAN & ADAM LAMPARELLO IN SUPPORT OF NEITHER PARTY

James J. Berles
Counsel of Record
Charles E. MacLean &
Adam Lamparello
Assistant Professors of Law
Indiana Tech Law School
1600 E. Washington Blvd.
Fort Wayne, IN 46803
1-855-TECHLAW

Library of Congress
Law Library

TABLE OF CONTENTS

Table of Authorities iii

Interest of Amici Curiae 1

Summary of Argument 3

Argument 8

I. Warrantless, Post-Arrest Searches of a Cell Phone are Unreasonable, and Not Justified by Any Exception to the Warrant Requirement 8

A. Individuals Have an Objectively Reasonable Expectation of Privacy in the Content of their Cell Phones 9

B. The Search Incident to Arrest Doctrine Does Not Support Warrantless, Post-Arrest Cell Phone Searches 14

1. Safety is Not a Concern 15

2. Evidence Will Not Be Destroyed 16

C. The Motor Vehicle Exception Does Not Support the Warrantless, Post-Arrest Search of a Cell Phone 17

II. The *Riley* Court Applied Old, Inapposite Doctrine to a New Problem, and the *Wurie* Court Did Not Provide the Necessary Exception for Exigent Circumstances 21

A. *People v. Riley* 21

B. *United States v. Wurie* 24

III. Allowing the Seizure of an Arrestee's Cell Phone, but Prohibiting its Warrantless Search Absent Exigent Circumstances, Preserves Law Enforcement's Interests and Protects Privacy 28

A. Remote Deletion is not a Sufficient Exigency 29

B. Imminent and Substantial Threats to Life and Safety are Sufficient Exigencies 30

C. The "Reasonable Relationship" Doctrine is Unworkable in the Cell Phone Context 32

D. The "Third Party Doctrine" is Unworkable in the Digital Age 32

IV. The Court's Rules in these Cases Will Drive Constitutional Jurisprudence for Decades No Matter Where the Digital Age Leads Us; It is Essential, therefore, that the Court Fashion a Broad Rule 34

Conclusion 37

TABLE OF AUTHORITIES

Cases **Page(s)**

Arizona v. Gant,
556 U.S. 332 (2009) ..... passim

California v. Acevedo,
500 U.S. 565 (1990) 9, 11

California v. Greenwood,
486 U.S. 35 (1988) 9

Chimel v. California,
395 U.S. 752 (1963) 3, 4, 7, 15, 22, 24

City of Ontario v. Quon,
560 U.S. 746 (2010) 27

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 19

Hudson v. Palmer,
468 U.S. 517 (1984) 9

Katz v. United States,
389 U.S. 347 (1967) 4, 9, 14, 24, 33-35

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013) 10-11, 26-27

Kyllo v. United States,
533 U.S. 27 (2001) 25

Lawrence v. Texas,
539 U.S. 558 (2003) 13

Maryland v. Buie,
494 U.S. 325 (1990) 18

Michigan v. Fisher,
558 U.S. 45 (2009) 31

Michigan v. Long,
463 U.S. 1032 (1983) 18

Mincey v. Arizona,
437 U.S. 385 (1978) 9

Missouri v. McNeely,
133 S. Ct. 1552 (2013) 8

New York v. Belton,
453 U.S. 454 (1981) 4, 5, 11, 15

Oliver v. United States,
466 U.S. 170 (1984) 3, 9

People v. Diaz,
244 P.3d 501(Cal. 2011) .....passim

People v. Riley, No. D059840, 2013 WL 475242,
(Cal. Ct. App. 4 Dist. Feb. 8, 2013) .....passim

Skinner v. Railway Labor Execs' Ass'n,
489 U.S. 602 (1989) 9

Smith v. Maryland,
442 U.S. 735 (1979) 18-19

Smith v. Ohio,
494 U.S. 541 (1990) 8-9

South Dakota v. Opperman,
428 U.S. 364 (1976) 9, 10

State v. Smith,
920 N.E.2d 949 (Ohio 2009) 4

Thornton v. United States,
541 U.S. 615 (2004) 5, 15, 20, 24, 26

United States v. Barone,
330 F.2d 543 (2d Cir. 1964), *cert. denied*,
84 S. Ct. 1940 (1964) 19

United States v. Chadwick,
433 U.S. 1 (1977) 9, 10

United States v. Edwards,
415 U.S. 800 (1974) 9, 23

United States v. Miller,
425 U.S. 435 (1976) 33

United States v. Park, No. CR 05–375 SI, 2007 WL
1521573 (N.D. Cal. May 23, 2007) 12

United States v. Jones,
132 S. Ct. 945 (2012) 25, 27

United States v. Place,
462 U.S. 696 (1983) 8-9

United States v. Robinson,
414 U.S. 218 (1973) 11, 23

United States v. Rodriguez,
995 F.2d 778 (7th Cir. 1993) 11

United States v. Ross,
456 U.S. 798 (1982) 17-18

United States v. Seiver,
692 F.3d 774 (7th Cir. 2012) 17

United States v. Seljan
547 F.3d 993 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 1368 (2009)..... 27

United States v. Wurie,
728 U.S. 1 (1st Cir. 2013) .....passim

Statutes

U.S. Const. amend. IV .....passim

Secondary Authorities

Samuel J. H. Beutler, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches*, 15 VAND. J. ENT. & TECH. L. 375 (2013) 3, 16-17, 29

Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307 (1998) 9-10

John P. Cronan, et al., *Fourth Amendment Trends and the Supreme Court's October 1999 Term*, 19 YALE L. & POL'Y REV. 197 (2000) 9-10

Mireille Dee, *Getting Back to the Fourth Amendment: Warrantless Cell Phone Searches*, 56 N.Y.L. SCH. L. Rev. 1129 (2012) 16

Joshua Eames, *Can You Hear Me Now? Warrantless Cell Phone Searches and the Fourth Amendment: People v. Diaz, 244 P.3d 501 (Cal. 2011)*, 12 WYO. L. REV. 483 (2012) 11

Clifford S. Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 65 RUTGERS L. REV. 995 (2013) 30, 31

David Goldman, *How police can find your deleted text messages*, CNN (May 22, 2013), *available at* http://money.cnn.com/2013/05/22/technology/mobile/smartphone-forensics/ 17

Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) 6

Jana L. Knott, *Is There an App for That? Reexamining the Doctrine of Search Incident to Lawful Arrest in the Context of Cell Phones*, 35 OKLA. CITY U. L. REV. 445 (2010) 11

Marty Koresawa, *Pay Phone Protections in a Smart Phone Society: The Need to Restrict Searches of Modern Technology Incident to Arrest*, 45 LOY. L.A. L. REV. 1351 (2012) 14-15

Adam Lamparello & Charles E. MacLean, *Back to the Future: Returning to Reasonableness and Particularity under the Fourth Amendment*, 99 IOWA L. REV. BULL. ___ (forthcoming 2014) 2

Charles E. MacLean, *But Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Searches of Cell Phone Memories Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37 (2012) 1

Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47 (2014) 1-2

Charles E. MacLean & Adam Lamparello, *Abidor v. Napolitano: Suspicionless Cell Phone and Laptop "Strip" Searches at the Border Compromise the Fourth and First Amendments*, 108 NW. U. L. REV. COLLOQUY ___ (forthcoming 2014) 2

Note, *Looking Back to Look Forward: Reexamining the Application of the Third-Party Doctrine to Conveyed Papers*, 37 HARV. J.L. & PUB. POL'Y 329 (2014) 24

Pew Research Internet Project, *Mobile Technology Facts Sheet, available at* http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ 7

Lily R. Robinton, *Courting Chaos: Conflicting Guidance From Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311 (2010) 13-14

Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489 (2012) 32-33

Ashley B. Snyder, Note, *The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155 (2011) 14

Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technologies*, 80 MISS. L.J. 1131 (2011) 34-35

INTEREST OF *AMICI CURIAE*

Amici Curiae Charles E. MacLean and Adam Lamparello[1] are assistant professors of law at Indiana Tech Law School in Fort Wayne, Indiana. They teach and write in the areas of criminal law, criminal procedure, and constitutional law, and have an interest in the sound development of the law in this area. They take the view that application of pre-digital age analogs and precedent to digital age technology is ill-advised and contrary to the Fourth Amendment, which, at a minimum, requires that searches be "reasonable" and enumerated with "particularity." Warrantless searches of digital storage devices, such as but not limited to smartphones, incident to lawful arrest, honor neither of those inviolable Fourth Amendment prongs.

Together or separately, *Amici* have written a number of articles regarding the application of the Fourth Amendment in the digital age, including: Charles E. MacLean, *But Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Searches of Cell Phone Memories Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37 (2012); Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age*

---

[1] All parties have consented to the filing of this amicus brief. No counsel for any party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the amici curiae, their law school, or their counsel made a monetary contribution to its preparation or submission.

Unless Congress Continually Resets the Privacy Bar, 24 ALB. L.J. SCI. & TECH. 47 (2014); Charles E. MacLean & Adam Lamparello, *Abidor v. Napolitano: Suspicionless Cell Phone and Laptop "Strip" Searches at the Border Compromise the Fourth and First Amendments*, 108 NW. U. L. REV. COLLOQUY ___ (forthcoming 2014); and Adam Lamparello & Charles E. MacLean, *Back to the Future: Returning to Reasonableness and Particularity under the Fourth Amendment*, 99 IOWA L. REV. BULL. ___ (forthcoming 2014).

SUMMARY OF ARGUMENT

Warrantless searches of cell phone memory—*after* a suspect has been arrested, and *after* law enforcement has seized the phone—would have been unconstitutional at the time the Fourth Amendment was adopted, and are unconstitutional now. Simply stated, they are unreasonable. And reasonableness—not a categorical warrant requirement—is the "touchstone of Fourth Amendment analysis." *Oliver v. United States*, 466 U.S. 170, 177 (1984).

Searches of a cell phone's contents cannot be justified under the search incident to arrest doctrine because neither safety nor the preservation of evidence is implicated. *See Arizona v. Gant*, 556 U.S. 332, 339 (2009) (citing *Chimel v. California*, 395 U.S. 752, 763 (1963)). To be sure, after seizure by law enforcement, cell phones are no longer part of the "arrestee's person" or within the arrestee's "immediate control." *Id.* Furthermore, there is minimal risk of automatic or remote deletion.[2] Thus, "application of *Chimel* in this context should be entirely abandoned." *Gant*, 556 U.S. at 354 (Scalia, J., concurring).

---

[2] *See, e.g.*, Samuel J. H. Beutler, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches*, 15 VAND. J. ENT. & TECH. L. 375, 394 (2013). (explaining that, "for an arrestee to effectively erase evidence ... (1) a phone must be enabled with remote wipe capabilities, (2) an accomplice must have access to the remote wipe program, and (3) there must exist some way for the arrestee to contemporaneously alert the accomplice of the arrest").

In addition, these searches are not supported by the vehicle inventory exception. Modern cell phones are not "articles inside the relatively narrow compass of the passenger compartment of an automobile," and *after* seizure by law enforcement are not within "the area into which an arrestee might reach.' " *Gant*, 556 U.S. at 341 (quoting *New York v. Belton*, 453 U.S. 454, 460 (1981)). They are in the hands of law enforcement. Not getting a warrant in this situation makes a mockery of the warrant requirement, its exceptions, and the reasonableness standard.

Cell phones are the modern day repository for the "papers" and "effects" that were stored in Eighteenth Century Colonial, Nineteenth Century Gothic Revival, and Twentieth Century Cape Cod homes. They store private correspondence, photographs, *personal thoughts*, and in some cases even the personal information of others. *See State v. Smith*, 920 N.E.2d 949, 954 (Ohio 2009). Within each "room" of a cell phone, individuals have an objective—and subjective—expectation of privacy against unreasonable searches and seizures. *See Katz v. United States*, 389 U.S. 347 (1967).

Given the recent advances in modern technology, the incompatibility with this Court's precedent, and the system-wide infringements that have occurred since *Belton*, the time has arrived to create a bright-line rule. As the Court recognized in *Gant*, "lower court decisions seem now to treat the ability to search a vehicle incident to the arrest of a recent occupant as a police entitlement rather than as an exception justified by the twin rationales of *Chimel*."

Gant, 556 U.S. at 342 (quoting *Thornton v. United States*, 541 U.S. 615, 624 (2004)) (O'Connor, J., concurring). Indeed, some courts have upheld searches under *Belton* "even when . . . the handcuffed arrestee has already left the scene." *Id.* (quoting *Thornton*, 541 U.S. at 629 (O'Connor, J., concurring)). That same entitlement prevails in the context of post-arrest, post-seizure cell phone searches. It should stop now, or cell phone searches may become the modern day general warrant. In some cases—such as *Riley*—they already have.

Relying on precedent from an era of black-and-white televisions would allow this practice to continue, and would stretch the search incident to arrest doctrine "beyond its breaking point." *Thornton*, 541 U.S. at 620, 625 (Scalia, J. concurring); *see also People v. Diaz*, 244 P.3d 501, 516-17 (Cal. 2011)) (Werdegar, J., dissenting) ("[t]he United States Supreme Court's holdings on clothing and small spatial containers were not made with mobile phones, smartphones and handheld computers—none of which existed at the time—in mind"). Indeed, the Court has "never relied on *stare decisis* to justify the continuance of an unconstitutional police practice . . . that is so easily distinguished from the decisions that arguably compel it." *Gant*, 556 U.S. at 348.

Professors MacLean and Lamparello respectfully submit that the Court should adopt a rule allowing law enforcement to seize an arrestee's cell phone, but prohibiting a search of its contents without probable cause and a warrant describing with particularity

the "rooms" to be searched.[3]

The only exception should be where law enforcement officers are faced with an *imminent* threat to life or safety.[4] Even then, however, the search should be proportionate to the nature and duration of the exigency, and not as a pretext to go on a fishing expedition for evidence of any crime whatsoever. Absent an exigent circumstance, searches of cell phone contents should be *ipso facto* unreasonable. The modest inconvenience to law enforcement is a small price to pay to prevent the unconstitutional infringements upon privacy that result when law enforcement officers, without a warrant, search cell phones incident to arrest.

---

[3] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) (discussing the particularity requirement in the context of internet searches). When either a search warrant or an exigency allows a law enforcement officer to "search" a cell phone, neither should occur without specifically enumerating the particular parts or "rooms" of the cell phone the officer is authorized to search. Just as an officer cannot constitutionally look inside an envelope when the officer is only authorized by the warrant or exigency to look for a stolen automobile, nor should any computer or cell phone "search" ever authorize a blunderbuss search of the entirety of its memory, that is, a search of all its "rooms," without regard to whether the probable cause provided sufficient justification and nexus for all of those "rooms." Both the "particularity" and the "reasonableness" prongs of the Fourth Amendment compel that particularity, without which the search cannot be deemed reasonable.

[4] Whether this requires an exception in every case is a separate issue.

Professors MacLean and Lamparello also counsel against carving out a narrow exception where officers have "reason to believe evidence relevant to the crime of arrest" will be found in the phone. *Gant*, 556 U.S. at 341 (quoting *Chimel*, 395 U.S. at 763). Such standard would not "provide the needed guidance to arresting officers," and would leave "much room for manipulation." *Gant*, 556 U.S. at 353 (Scalia, J., concurring). That distinction threatens to swallow the rule and is a recipe for arbitrariness of the most unreasonable—and unconstitutional—kind.

Ultimately, there can be no doubt—in an era of unprecedented technological advances—that individual privacy is under attack by state action that neither the Fourth Amendment nor basic notions of liberty countenance. Smartphones are now owned and operated by fifty-five percent of the population[5] and transcend the finite physical space that is traditionally subject to searches incident to arrest or other exceptions to the warrant requirement. Warrantless, post-arrest searches of cell phones therefore implicate privacy interests that the Fourth Amendment, at the time of its adoption and throughout its evolution, safeguards against arbitrary government intrusion. These searches are unnecessary, unreasonable, and unconstitutional.

---

[5] *See, e.g.*, Pew Research Internet Project, *Mobile Technology Facts Sheet, available at* http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

ARGUMENT

I. WARRANTLESS, POST-ARREST SEARCHES OF A CELL PHONE ARE UNREASONABLE AND NOT JUSTIFIED BY ANY EXCEPTION TO THE WARRANT REQUIREMENT.

The Fourth Amendment does not categorically require a warrant. It demands reasonableness.[6] And a "warrantless search of the person is reasonable only if it falls within a recognized exception." *Missouri v. McNeely*, 133 S. Ct. 1552, 1558 (2013). Warrantless searches of cell phones fall within no exception. And for good reason. They offend even the most relaxed definition of reasonableness.

In *Smith v. Ohio*, the Court explained that "[a]lthough the Fourth Amendment may permit a brief *detention* of property on the basis of only 'reasonable, articulable suspicion' that it contains contraband or evidence of criminal activity, it proscribes—except in certain well-defined circumstances—the search of that property unless accomplished pursuant to judicial warrant issued upon probable cause." 494 U.S. 541, 542 (1990)

---

[6] *See* U.S. Const. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized").

(*quoting United States v. Place*, 462 U.S. 696, 702 (1983)); *see also Skinner v. Railway Labor Execs' Ass'n*, 489 U.S. 602, 619 (1989); *Mincey v. Arizona*, 437 U.S. 385, 390 (1978); *Katz*, 389 U.S. at 357. A brief discussion of the character of cell phones demonstrates that they do not fall within the warrant requirement's "established and well-delineated exceptions." *Katz*, 389 U.S. at 357.

A. Individuals Have an Objectively Reasonable Expectation of Privacy in the Content of their Cell Phones.

Cell phones are unlike any of the objects that this Court has confronted in its jurisprudence. *See, e.g., California v. Greenwood*, 486 U.S. 35, 40 (1988) (trash left on the curb); *Oliver*, 466 U.S. 170 (objects or activities in open fields) (1984); *Hudson v. Palmer*, 468 U.S. 517 (1984) (items in prison cells); *United States v. Chadwick*, 433 U.S. 1 (1977) (footlocker), *abrogated by California v. Acevedo*, 500 U.S. 565 (1990); *South Dakota v. Opperman*, 428 U.S. 364 (1976) (cars); *United States v. Edwards*, 415 U.S. 800 (1974) (clothing).

The above cases establish three levels or gradations of privacy. First, privacy expectations "that society is prepared to recognize as legitimate have, at least in theory, the greatest protection." John P. Cronan, et al., *Fourth Amendment Trends and the Supreme Court's October 1999 Term*, 19

YALE L. & POL'Y REV. 197, 200 (2000) (quoting Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 331 (1998)) (internal quotations and footnotes omitted). Houses, for example, fall within this group. Cronan, *supra*, at 200. Areas where an individual has "diminished expectations of privacy are more easily invaded." *Id.* (*quoting* Clancy, *supra*, at 331). Cars have been placed in this group. *Opperman*, 428 U.S. at 367. Finally, "subjective expectations of privacy that society is not prepared to recognize as legitimate have no protection." Cronan, *supra*, at 200 (*quoting* Clancy, *supra*, at 331).

Cell phones deserve the highest privacy protections. They transcend physical boundaries and finite space, shatter the distinctions between public thoroughfares and private homes, and store the "papers" and "effects" that, in the pre-digital era, were kept in the privacy of one's home. These items are not rendered searchable simply because they are stored in a cell phone rather than a closet. *See Chadwick*, 433 U.S. at 13. ("the footlocker's mobility [does not] justify dispensing with the added protections of the Warrant Clause").

That principle applies with particular force here. In the cell phone context, mobility and location are less relevant. The more pertinent inquiry should focus on the diverse array of deeply personal contents that can—and are—stored within cell phones, as well as the ubiquity of cell phones in contemporary life. As one court aptly described, we now live in a "cell-

phone centric" society. *Klayman v. Obama*, 957 F. Supp. 2d 1, 36 (D.D.C. 2013).

Cell phones cannot be analogized to a crumpled up cigarette package, address book, wallet, or container. *See Robinson*, 414 U.S. at 236; *United States v. Rodriguez*, 995 F.2d 778, 778 (7th Cir. 1993); *Acevedo*, 500 U.S. at 575-76. That would be like comparing a rotary telephone to a Smartphone.

Unlike a container, for example, a cell phone is not an "object capable of holding another object." *Belton*, 453 U.S. at 460 n.4. Moreover, cell phone contents are "limited to digital data, the intangible nature of which renders it unavailable for use as a weapon or as evidence that can be physically destroyed." Joshua Eames, *Can You Hear Me Now? Warrantless Cell Phone Searches and the Fourth Amendment; People v. Diaz, 244 P.3d 501 (Cal. 2011)*, 12 WYO. L. REV. 483, 499 (2012).

Also, "modern cell phones are capable of accessing almost limitless amounts of data," and "[e]ven the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container." *Id.; see also* Jana L. Knott, *Is There an App for That? Reexamining the Doctrine of Search Incident to Lawful Arrest in the Context of Cell Phones*, 35 OKLA. CITY U. L. REV. 445, 456 (2010).

But it is the quality, not simply the quantity, of data that distinguishes cellphones from parked cars, passenger compartments, pagers, and plastic containers:

> [M]odern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.

United States v. Park, No. CR 05–375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007). ("[a]lthough information of this nature can now be stored electronically, in the past such information has traditionally been stored in one's home office or desk and given protection by the Fourth Amendment"). Put differently, people do not store confidential documents in a Rolodex, and they do not watch YouTube videos in a suitcase.

As such, relying on cases from an era of rotary phones and black-and-white televisions is akin to relying on the plain view doctrine to justify pulling apart the curtains of someone's home to get a glimpse into their private life. While precedent is vital to ensuring predictability and consistency, it has less importance in this case. And stare decisis "does not compel us to follow a past decision when its

rationale no longer withstands 'careful analysis.'" *Gant*, 556 U.S. at 348 (quoting *Lawrence v. Texas*, 539 U.S. 558, 577 (2003)).

The "potential intrusion on informational privacy involved in a police search of a person's mobile phone, smartphone, or handheld computer," is substantial. *Diaz II*, 244 P.3d at 513 (Werdegar, J., dissenting). The justifications for searching these items without a warrant, however, are not. Noting that the amount of information that can be stored on a cell phone "dwarfs that which can be carried on the person in a spatial container," Judge Werdegar criticized the *Diaz* majority for "indulg[ing] a fiction that an item that was on the arrestee's person when he was detained is *still* on his person—and thus vulnerable to destruction of evidence—notwithstanding that the arrestee is safely in custody and the item securely in police control." *Id.* at 515.

The threats to privacy are particularly acute because cell phones have become "attractive targets for criminal investigators, providing a wealth of evidence such as lists of recent incoming and outgoing calls, text messages, and possibly incriminating photographs." Lily R. Robinton, *Courting Chaos: Conflicting Guidance From Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 315 (2010); Ashley B. Snyder, Note, *The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 163 (2011). To make matters worse, law enforcement can search for incriminating evidence by "just 'thumbing through'

the cell phone." Snyder, *supra* at 163.

Not only does this "increase the likelihood that highly personal information that is irrelevant to the subject of the lawful investigation will also be searched," but it also demonstrates the reasonableness, under *Katz*, of finding that an individual has a constitutionally protected expectation of privacy in cell phones. And it underscores the unreasonableness of searching cell phones unless law enforcement has a warrant, or is confronted with an exigent circumstance.

B. THE SEARCH INCIDENT TO ARREST DOCTRINE DOES NOT SUPPORT WARRANTLESS, POST-ARREST CELL PHONE SEARCHES.

As the Court stated in *Gant*, the "the scope of a search incident to arrest is commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy." 556 U.S. at 339. A cell phone implicates neither of these concerns—particularly after it is seized.

1. Safety is Not a Concern.

A cell phone is not—and cannot—be used as a weapon,[7] and "cannot hide weapons."[8] Thus, the

---

[7] *See e.g.*, Marty Koresawa, *Pay Phone Protections in a Smart Phone Society: The Need to Restrict Searches of Modern Technology Incident to Arrest*, 45 LOY. L.A. L. REV. 1351, 1389

distinctions established in search incident to arrest jurisprudence, including "immediate control," and "lunging area," which were driven by safety concerns, do not apply in the cell phone search context. *Gant*, 556 U.S. at 339 (*quoting Chimel*, 395 U.S. at 763); *Diaz II*, 244 P.3d at 505. In *Gant*, Justice Scalia stated as follows:

> Since the historical scope of officers' authority to search vehicles incident to arrest is uncertain . . . traditional standards of reasonableness govern. It is abundantly clear that those standards do not justify what I take to be the rule set forth in *New York v. Belton* . . . and *Thornton*: that arresting officers may always search an arrestee's vehicle in order to protect themselves from hidden weapons. When an arrest is made in connection with a roadside stop, *police virtually always have a less intrusive and more effective means of ensuring their safety—and a means that is virtually always employed: ordering the arrestee away from the vehicle, patting him down in the open, handcuffing him, and placing him in the squad car*

Gant, 556 U.S. at 351-52 (Scalia, J., concurring).

(2012).

[8] *Id.* at 1389.

The same "less intrusive" means are available in the cell phone context. Police can seize the phone, and subsequently procure a warrant to search its contents.

2. Evidence Will Not Be Destroyed.

The only issue that ever arguably arises in a cell phone memory search context relates to the preservation of evidence. Importantly, however, unless an arrestee's cell phone has minimal storage capacity, an automatic delete function, or can be remotely deleted by a third party, the risk of losing evidence is remote.[9]

Modern cell phones "no longer store only a handful of recent text messages and phone calls and greatly expanded digital memories eradicate any real risk of automatic deletion."[10] Also, even though remote deletion "pose[s] a real and substantial risk of destroying evidence,"[11] it depends on factors that law enforcement can mitigate by *seizing*—but not *searching*—the phone. As one commentator explains, "for an arrestee to effectively erase evidence . . . (1) a phone must be enabled with remote wipe capabilities, (2) an accomplice must have access to the remote wipe program, and (3) there must exist some way for the arrestee to *contemporaneously alert*

---

9 *See* Mireille Dee, *Getting Back to the Fourth Amendment: Warrantless Cell Phone Searches,* 56 N.Y.L. SCH. L. Rev. 1129, 1152 (2012).

10 *See, e.g.*, Beutler, *supra* note 2, at 394.

11 *Id.* at 395.

the accomplice of the arrest."[12] And even wiped data can often be forensically recovered.[13]

C. The Motor Vehicle Exception Does Not Support the Warrantless, Post-Arrest Search of a Cell Phone.

The Court has set forth several instances when a vehicle may be searched without a warrant. The first "permit[s] an officer to conduct a vehicle search when an arrestee is within reaching distance of the vehicle or it is reasonable to believe the vehicle contains evidence of the offense of arrest." *Gant,* 556 U.S. at 346. An officer may also search a "vehicle's passenger compartment when he has reasonable suspicion that an individual, whether or not the arrestee, is 'dangerous' and might access the vehicle to "gain immediate control of weapons." *Gant,* 556 U.S. at 346-47 (quoting *Michigan v. Long,* 463 U.S. 1032, 1049 (1983)).

Additionally, a warrantless search of the entire vehicle is permissible if "there is *probable cause* to believe a vehicle contains evidence of criminal activity." *Gant,* 556 U.S. at 347 (*citing United States*

---

[12] *Id.* (emphasis added).

[13] *See* David Goldman, *How police can find your deleted text messages,* CNN (May 22, 2013), *available at* http://money.cnn.com/2013/05/22/technology/mobile/smartphone-forensics/; *see also United States v. Seiver,* 692 F.3d 774, 776 (7th Cir. 2012) (deleted file recovery in a computer context).

v. Ross, 456 U.S. 798, 820–21 (1982)) (emphasis added); *see also Maryland v. Buie*, 494 U.S. 325, 334 (1990) (a limited protective sweep of a home is permissible in areas where an officer believes a dangerous person may be hiding). Finally, although *Ross* authorizes even broader searches for "evidence relevant to offenses other than the offense of arrest," it is intended to safeguard "*genuine* safety or evidentiary concerns" encountered during the arrest of a vehicle's recent occupant. *Gant*, 556 U.S. at 347 (emphasis added).

Proffered concerns about safety or preserving evidence in cell phone searches incident to arrest are not credible. They are pretext to go on a fishing expedition. Based on the quantity and quality of private information stored in cell phones, law enforcement has virtually unlimited access to an arrestee's private life, including confidential communications in a personal or professional setting, intimate messages to family members and loved ones, and internet search history. Furthermore, the only event that triggers such a search is the arrest itself, regardless of whether it is for Driving under the Influence of Alcohol or Premeditated Murder. And it is not intended to protect officer safety, preserve evidence, or even search for evidence relating to the crime of arrest. It is to search for any evidence of any crime in any *room* that law enforcement desires. In a nutshell, that is the essence of a general warrant.

To be sure, it is one thing to use a pen register to track a suspect's outgoing calls from a private residence. *See Smith v. Maryland*, 442 U.S. 735

(1979) (holding that law enforcement could use a pen register to track outgoing telephone calls from a suspect's private residence). It is quite another to go on a fishing expedition for evidence of any crime, particularly when there are no reasons to justify the search, and nothing to prevent law enforcement from seizing the phone and subsequently obtaining a warrant. There is nothing reasonable about this practice.

And reasonableness is the foundation for every exception to the warrant requirement. Under the public safety exception, for example, it is reasonable to allow officers to forego a search warrant prior to entering a building where they hear screams for help as they approach. *See United States v. Barone*, 330 F.2d 543, 544-45 (2d Cir. 1964), *cert. denied*, 84 S. Ct. 1940 (1964)). A plain view search is likewise reasonable; the officers had a right to be present where they saw the inculpating item in plain view, thus we need not call it a "plain view" search – under the Constitution, it is a reasonable search – the "plain view" label is just veneer. *See Coolidge v. New Hampshire*, 403 U.S. 443, 464-69 (1971).

On the other hand, it is not reasonable to conduct a warrantless search of a cell phone's memory merely because it was in the arrestee's pocket. The officer's safety is not threatened. There is little, if any, risk that the information will be deleted. Thus, relying on the "search incident to arrest" exception in this context is not merely stretching the doctrine "beyond its breaking point"; it is stretching reasonableness to a place that this Court should not be willing to go.

Thornton, 541 U.S. at 625 (Scalia, J. concurring).

Ultimately, the reason this Court has not endorsed a categorical warrant requirement is identical to that which gave rise to the above exceptions: it was reasonable to do so. Searching cell phones without a warrant or demonstrable exigency fails to satisfy this standard.

II. THE *RILEY* COURT APPLIED OLD, INAPPOSITE DOCTRINE TO A NEW PROBLEM, AND THE *WURIE* COURT DID NOT PROVIDE THE NECESSARY EXCEPTION FOR EXIGENT CIRCUMSTANCES.

A. *People v. Riley.*

In *People v. Riley*, the California Court of Appeals followed *Diaz*,[14] and upheld the warrantless search of defendant's cell phone because it was, "immediately associated with his person when he was arrested, and therefore the search of his cell phone was lawful whether or not an exigency still existed." *See People v. Riley*, No. D059840, 2013 WL 475242, at *6 (Cal. Ct. App. 4 Dist. Feb. 8, 2013), unpublished/noncitable, *review denied* (May 01, 2013), *cert. granted in part*, Riley v. California, ___ S. Ct. ___, No. 13-132, 2013 WL 3938997, 82 U.S.L.W. 3082 (Jan. 17, 2014). The California Court of Appeals reached the wrong result. The search was unlawful because it was not reasonable.

Even if the cell phone was immediately associated with Riley's "person," it neither threatened the officers' safety nor presented a risk that evidence would be destroyed. Tellingly, the Court of Appeals made no attempt to establish a

---

[14] 81 Cal. Rptr. 3d 732 (Cal. Ct. App. 2008) ("*Diaz I*"), *aff'd*, 244 P.3d 501 (Cal. 2008) ("*Diaz II*"); *cert. denied sub. nom., Diaz v. California*, 132 S. Ct. 94 (Oct. 3, 2011).

nexus between the *Chimel* justifications and the subsequent search of Riley's cell phone. Instead, the California Court of Appeals permitted an unfettered search of Riley's cell phone, essentially sanctioning a suspicionless fishing expedition into his personal life. As Judge Werdegar noted in his dissent, the majority's decision "sanctions a highly intrusive and unjustified type of search, one meeting neither the warrant requirement nor the reasonableness requirement of the Fourth Amendment to the United States Constitution." 244 P.3d at 518.

In doing so, the California Court of Appeals failed to make an important distinction between the privacy interests at stake. And that distinction is what lies at the heart of this case. The individual's expectation of privacy is not in a cell phone *as an object*, but as the safe keeper of the "papers" and "effects" that the Fourth Amendment has *always* deemed private. *See Diaz,* 244 P.3d at 517 (Werdegar, J., dissenting) ("the grounds for deeming an arrestee to have lost privacy rights in his or her *person* do not apply to the privacy interest in *data* stored on electronic devices"). In *Diaz,* Judge Werdegar explained as follows:

> In *Robinson,* the Supreme Court . . . explained that while warrantless searches of the person are ordinarily unlawful, [s]earch of the person becomes lawful when grounds for arrest and accusation have been discovered, and *the law is in the act of subjecting the body of the accused to its physical dominion* . . . It does not follow,

> however, that the police also have "'dominion . . . over the entirety of stored messages, photographs, videos, memoranda and other records an arrestee may be carrying on a mobile phone or smartphone. That an arrestees interest in his or her own privacy' " . . . is severely reduced does not imply a corresponding reduction in privacy of personal and business data. Even when they happen to be stored on a device carried on the person, these records are clearly distinct from the person of the arrestee.

Id. at 517-18 (Werdegar, J., dissenting) (*quoting Robinson,* 414 U.S. at 232; *Edwards,* 415 U.S. at 809). Put differently, "[a]n individual lawfully arrested and taken into police custody necessarily loses much of his or her *bodily* privacy, but does not necessarily suffer a reduction in the *informational* privacy that protects the arrestee's records." *Id.* at 517.

Surely, an individual has at least *some* expectation of privacy in personal documents stored on a cell phone, videos downloaded from YouTube, or private emails sent from an email account. While this does not immunize the information from a valid search, it does require law enforcement to have probable cause and a warrant—or sufficient justification for proceeding under one of the exceptions to the warrant requirement—before rummaging through such private space.

In *Riley,* law enforcement had neither, and the California Court of Appeals' "fanciful reliance upon

officer safety [should be recognized] for what it was: "a return to the broader sort of [evidence-gathering] search incident to arrest that we allowed before *Chimel*." *Thornton*, 541 U.S. at 631 (Scalia, J., concurring).

Of course, there is nothing problematic about saying that a cell phone is "immediately associated" with the person, if this term is construed as an association with the person's thoughts, private "papers," and personal "effects." Note, *Looking Back to Look Forward: Reexamining the Application of the Third-Party Doctrine to Conveyed Papers*, 37 HARV. J.L. & PUB. POL'Y 329, 330 (2014).

In *Wurie*, however, the First Circuit got it right, cell phone data searches are *categorically* unlawful under the search incident to arrest exception, given the government's failure to demonstrate that they are ever necessary to promote officer safety or prevent the destruction of evidence. *See Katz*, 389 U.S. at 353.

B. *United States v. Wurie*.

The First Circuit's decision in *Wurie* drew a better, but not sufficiently brighter, line. The Court recognized that unrestricted searches of an arrestee's cell phone were anything but reasonable:

> Since the time of its framing, "the central concern underlying the Fourth Amendment" has been ensuring that

> law enforcement officials do not have "unbridled discretion to rummage at will among a person's private effects" . . . Today, many Americans store their most personal "papers" and "effects," in electronic format on a cell phone, carried on the person. Allowing the police to search that data without a warrant any time they conduct a lawful arrest would, in our view, create "a serious and recurring threat to the privacy of countless individuals."
>
> * * *
>
> In reality, "a modern cell phone is a computer," and "a computer . . . is not just another purse or address book."

728 U.S. 1, 8, 14 (1st Cir. 2013) (internal citations omitted); *see also United States v. Jones*, 132 S. Ct. 945, 950 (2012) ("[a]t bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted'") (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

The First Circuit also recognized that the information stored on cell phones is the type of "information one would previously have stored in one's home and that would have been off-limits to officers performing a search incident to arrest."

Wurie, 728 U.S. at 8. The court stated as follows:

> Just as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government's proposed rule [allowing searches of cell phone memories as a bright-line rule] would give law enforcement automatic access to "a virtual warehouse" of an individual's "most intimate communications and photographs without probable cause" if the individual is subject to a custodial arrest, even for something as minor as a traffic violation.

Id. at 8-9.

Finally, the First Circuit flatly rejected the search incident to arrest justification, holding that "warrantless cell phone data searches strike us as a convenient way for the police to obtain information related to a defendant's crime of arrest – or other, as yet undiscovered crimes – without having to secure a warrant." *Id.* at 12-13. As the court correctly noted, "nothing in the Supreme Court's search-incident-to-arrest jurisprudence that sanctions such a general evidence-gathering search." *Id.* (quoting *Thornton* 541 U.S. at 632 (Scalia, J., concurring)).

More recently, in *Klayman,* the United States District Court for the District of Columbia held that

the National Security Agency's ("NSA") surveillance program, which consisted of the suspicionless collection of cell-phone metadata, likely constituted a search under the Fourth Amendment. 957 F. Supp. 2d at 37. In so holding the court explained that, because "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago," the Government "metadata collection and analysis almost certainly does violate a reasonable expectation of privacy." *Id.* at 32, 36. The court recognized the "rapid and monumental shift towards a cell-centric culture," where metadata from each person's phone reveals " 'a wealth of detail about her familial, political, professional, religious, and sexual associations.' *Id.* at 36 (quoting *Jones*, 132 S. Ct. at 955-56). As this Court noted in *City of Ontario v. Quon*, "[t]hat might strengthen the case for an expectation of privacy." 560 U.S. 746, 760 (2010).

It does strengthen the case because times have changed. So too should this Court's view of privacy in the cell phone search context, which implicates privacy in ways that pre-digital case law could not foresee. *See United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, J., dissenting), *cert. denied*, 129 S. Ct. 1368 (2009) ("[t]he reference to papers [in the Fourth Amendment] is not an accident; it's not a scrivener's error. It reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas--what we might call freedom of conscience--from invasion by the government"). Searching a cell phone's memory is, in essence, searching persons *and* their "papers," memories, thoughts, and historical locations. It gives

law enforcement license to forage through an individual's private life—and *mind*—where less intrusive methods are available to safeguard law enforcement's evidence gathering function.

III. ALLOWING THE SEIZURE OF AN ARRESTEE'S CELL PHONE, BUT PROHIBITING ITS WARRANTLESS SEARCH ABSENT EXIGENT CIRCUMSTANCES, PRESERVES LAW ENFORCEMENT'S INTERESTS AND PROTECTS PRIVACY.

Professors MacLæan and Lamparello respectfully submit that the pragmatic approach would be to: (1) allow law enforcement to seize an arrestee's cell phone; (2) require a warrant and probable cause to search the phone's contents; and (3) provide a narrow exception for imminent substantial threats to human life and safety. This standard would bring more certainty and guidance in a jurisprudence that is currently unsettled. *See Diaz*, 51 Cal. 4th at 518 (Werdegar, J., dissenting) (instead of searching an arrestee's cell phone without a warrant, "the item can be taken from the arrestee and securely held until (assuming probable cause for a search exists) a warrant has issued").

In *Gant*, the Court inched in this direction when it held that a motor vehicle search incident to arrest was improper. 556 U.S. at 351-52. The Court recognized that, because the officers' safety was not at risk, and, because they had no reason "to believe evidence relevant to the crime of arrest might be found in the vehicle," there was no justification for

the search. The same is true here.

The time has come for a bright-line rule recognizing that individuals have an objectively reasonable expectation of privacy in the contents of their cell phones. That means the following: seizing the phone is permissible because it would prevent an arrestee from destroying evidence, coordinating with third parties to endanger officer safety, or remotely deleting the cell phone's memory. On the other hand, searching it without a warrant and probable cause, "would give authorities an open door into the most private details of an arrestee's life."[15] The only exception is when officers are faced with exigent circumstances. But the Court must also define the contours of this exception, so that it is not used to circumvent the rule.

A. *Remote Deletion is not a Sufficient Exigency.*

As discussed above, "[r]apid improvements in technology . . . have obviated the . . . concern[]" that "incoming calls or messages will replace recent calls or messages in a phone's memory." Beutler, *supra* note 2, at 394. Riley, Wurie, and other *Amici* have covered this issue at length. Remote deletion is such an attenuated risk, that it cannot suffice to justify a warrantless cell phone memory search incident to arrest.[16]

---

[15] *Id.* at 1064.

[16] Even where officers are aware of an actual and specific risk of remote deletion, that risk can be obviated by the simple and

B. *Imminent and Substantial Threats to Life and Safety are Sufficient Exigencies.*

Where law enforcement officers have an objectively reasonable belief that an "immediate threat to [human] life or safety" exists, they should be entitled to search a cell phone without a warrant, limited to the areas ("rooms") in the cell phone where evidence relevant to the exigency itself could reasonably be found. Clifford S. Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 65 RUTGERS L. REV. 995, 1002 (2013); *see also Michigan v. Fisher*, 558 U.S. 45, 47 (2009); *Diaz*, 244 P.3d at 518 (Werdegar, J., dissenting) ("where the arresting officers have reason to fear imminent loss of evidence from the device, or some other exigency makes immediate retrieval of information advisable, warrantless examination and search of the device would be justified").

One scholar explains the exigent circumstances exception as follows:

> [P]olice may enter premises and conduct a search without a warrant "to provide emergency assistance to an occupant," or to "enter a burning building to put

---

inexpensive safeguards available today (for example, turn the phone off, remove its battery, place the phone in a Faraday enclosure, or make a mirror image of the phone's memory for subsequent search only *if and when* the officers obtain a search warrant).

> out a fire and investigate its cause." In such cases, the law not only dismisses the warrant requirement--in appropriate circumstances, the police may act even in the absence of probable cause.

Fishman, *supra* at 1003. Furthermore, to prevent the exception from swallowing the rule, law enforcement should be required to show that it had a reasonable belief that the exigency presented an imminent and substantial threat to the life or physical safety of others. While law enforcement does not need "ironclad" proof of an exigency, the Court should require that it does not encompass any threat, no matter how attenuated or speculative. *Fisher*, 558 U.S. at 49. The belief must be reasonable—as the Fourth Amendment requires.

It should also be sufficiently particular. A constitutional search pursuant to such an exigency must be limited to areas within the cell phone that are likely to uncover evidence relating to the exigency. In some situations, this may include initiating or responding to a call or text message, or reviewing the arrestee's recent phone calls or emails. Fishman, *supra* at 1004-05. It should not, for example, give officers license in every case to search the arrestee's Google search history or purchases on Amazon.com. Additionally, the search must cease when the exigency dissipates, or when officers discover evidence—in the cell phone or elsewhere—that allows them to effectively address the problem.

C. *The "Reasonable Relationship" Doctrine is Unworkable in the Cell Phone Context.*

What worked in *Gant*—which involved the search of an automobile—does not work when applied to cell phones. In other words, searches should not be allowed simply because the cell phone may contain evidence related to the crime of arrest. *See Gant*, 556 U.S. at 351. A cell phone stores far more information than can be found in a passenger compartment, a trunk, or a few closed containers.

Thus, the risk that officers will simply rummage through all "rooms" of the cell phone in an unfettered search for evidence far outweighs the convenience to law enforcement. Furthermore, given the minimal, even non-existent, risk that a cell phone's memory will be destroyed, there exist no reasons whatsoever that could justify such a warrantless search. Requiring officers to, instead, procure a warrant will allow a magistrate judge to confine the scope of every search, and describe with particularity the areas of a cell phone that are properly subject to a search.

D. *The "Third Party Doctrine" is Unworkable in the Digital Age.*

Some courts have relied on the third-party doctrine to hold that a cell phone user's Google searches and sent emails constitute a voluntary disclosure (thus surrendering Fourth Amendment protections), because the user knows that the search or email will be transmitted through a server. Jeremy H. Rothstein, *Track Me Maybe: The Fourth*

Amendment and the Use of Cell Phone Tracking to Facilitate Arrest, 81 FORDHAM L. REV. 489, 506 (2012) (discussing United States v. Miller, 425 U.S. 435, 442-43 (1976)).

Importantly, however, "the Supreme Court decisions that established the third-party doctrine are decades old," and cell phones, just as they are not containers or address books, are unlike "bank records voluntarily conveyed to banks in the ordinary course of business." *Id.* at 507-08 (discussing *Miller*, 425 U.S. at 442-43). They are also not comparable to "exposing numerical information to the telephone company," because individuals should not be required to "assum[e] the risk that the company would turn over that information to the government." *Id.* at 506.

If this reasoning were applied to cell phones, it would, in effect, condition the downloading and storage of traditionally private information, *e.g.*, confidential legal documents, upon the knowing waiver of constitutional rights. No conception of constitutional reasonableness can support this view, because it would result in an unconstitutional chill, through a *de facto* prior restraint, on speech and other expressive activity.

It would also require the assumption, under *Katz*, that individuals do not have an objectively reasonable expectation of privacy[17] in *otherwise-*

---

[17] *Katz* came to be seen as having held that the Fourth Amendment is triggered only where an individual can demonstrate both an objective and subjective expectation of privacy. 389 U.S. at 361-62 (Harlan, J., concurring).

private material simply because they know it may be viewed by an unidentified third party, for whatever reason, and disclosed to the government, for no reason. That logic might work for bank records that are given to tellers, or numbers that are dialed from a home phone. But it goes too far when applied to private information that reveals intimate details about individuals, and embraces a concept of disclosure that is incompatible with the role cell phones play in the digital age. Individuals using their cell phones to send text messages or emails, for example, are not 'disclosing' information in the traditional sense; they are capitalizing on the efficiency cell phones offer and the ubiquitous role they play in modern human interaction. Comparing a Google search to the act of handing over bank records to a teller fails to appreciate these differences, and ignores the fact the 'disclosure' in this context is not to a single person, but to the entire world. That requires more, not less, protection.

IV. THE COURT'S RULES IN THESE CASES WILL DRIVE CONSTITUTIONAL JURISPRUDENCE FOR DECADES NO MATTER WHERE THE DIGITAL AGE LEADS US; IT IS ESSENTIAL, THEREFORE, THAT THE COURT FASHION A BROAD RULE.

In the same way that *Katz* drove Fourth Amendment jurisprudence far beyond the phone booth,[18] the Court's decisions in these cases will

---

[18] As surveyed by Louisville Professor Russell Weaver, *Katz* has been applied to digital era cases as disparate as officer use

drive Fourth Amendment rights far beyond flip phones, iPhones, and any other snapshot of today's digital age technologies. It is, therefore, incumbent on the Court to issue a bright-line rule that provides clear guidance to law enforcement, and added protections for individuals.

The Court's decision will also guide lower courts for decades as they struggle with new factual scenarios brought about by rapid advances in technology. Just as pre-digital era case law could not foresee these developments, this Court also cannot know the numerous issues that will arise as technology continues to evolve. A broad and categorical rule will help to eliminate some of the uncertainty. A narrow rule would invite chaos.

To be sure, some courts, in considering cell phone searches incident to arrest, have focused on the particular features and capabilities of the type of cell

---

of flashlights, low-flying helicopters, aerial photography, radio transmitters, electronic listening devices, infrared technologies, and information conveyed through a third party. Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technologies*, 80 MISS. L.J. 1131, 1186-1221, 1227 (2011) ("today, more than three decades after *Katz* was decided, it is not clear that the Court's [reasonable expectation of privacy] test is providing [privacy] protections, or that the test is capable of doing so"). Professors MacLean and Lamparello suggest that perhaps now is the time for the Court to consider abandoning the "reasonable expectation of privacy" approach in favor of a "constitutional reasonableness" test, focused on the reasonableness of safeguarding the "persons, houses, papers, and effects" that officers choose to search and seize, and the reasonableness of the officers' actions in searching and seizing them, with or without a warrant.

phone before them. But this Court, issuing just 100 or so formal opinions per year, may not revisit the issues raised in *Riley* and *Wurie* for many years. Therefore, this decision must stand the test of time.

Professors MacLean and Lamparello suggest that the Court and society would be best served by decisions in *Riley* and *Wurie* that look beyond flip phones and iPhones. Perhaps denominating the rule as applicable to "digital storage devices,"[19] rather than to cell phones of this type or that, would be sufficient. Whatever rule is adopted, and whatever language employed, it should include a requirement that already has stood the test of time: reasonableness.

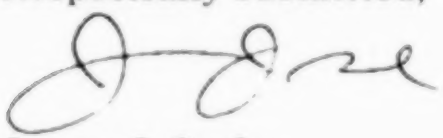
---

[19] Digital storage devices, as used here, could include digital data storage instruments capable of storing substantial quantities of the types of "papers" and "effects" protected by the Fourth Amendment, including cell phones, smartphones, laptop computers, tablet computers, thumb drives, external storage devices, DVDs, and the like as those technologies expand in the future.

CONCLUSION

For these reasons, and those set forth by Petitioner, the judgment in *Riley v. California* should be reversed, and the judgment in *United States v. Wurie* should be affirmed with the modifications addressed herein.

Respectfully submitted,



James J. Berles
Counsel of Record
Charles E. MacLean &
Adam Lamparello
Assistant Professors of Law
Indiana Tech Law School
1600 E. Washington Blvd.
Fort Wayne, IN 46850
1-855-TECHLAW
JJBerles@IndianaTech.edu
CEMacLean@IndianaTech.edu
AXLamparello@IndianaTech.edu

AMICUS CURIAE BRIEF

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
MAR 10 2014
OFFICE OF THE CLERK

No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari to the California Court of Appeal, Fourth District

BRIEF OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND THE BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW AS AMICI CURIAE IN SUPPORT OF PETITIONER

JEFFREY T. GREEN
CO-CHAIR, AMICUS COMMITTEE
NAT'L ASS'N OF CRIMINAL DEFENSE LAWYERS
1501 K Street, N.W.
Washington, D.C. 20005

BRONSON D. JAMES*
BRONSON JAMES LLC
522 N.W. 23rd Ave.
Portland, OR 97210
(503) 943-6876
bj@bronsonjames.com

MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
161 Ave. of the Americas,
New York, NY 10013

Counsel for Amici Curiae

* Counsel of Record

March 10, 2014

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

Library of Congress
Law Library

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	iii
INTEREST OF AMICI CURIAE	1
SUMMARY OF THE ARGUMENT	2
ARGUMENT	3
I. Mobile Computing Devices Like The Modern Smartphone Are Unique.	3
A. The Capacity Of Mobile Computing Devices Renders Analogies To Physical Containers Inapplicable	3
B. Mobile Devices Have Been Incorporated Into Modern Living In A Fundamentally Private And Personal Way.	6
C. The Smartphone Is The New Instrument Of First Amendment Expression	9
II. The Warrantless Search Of A Smartphone Incident To Arrest Is Not Justified Under The Search Incident To Arrest Doctrine	11
A. Neither Of The *Chimel* Rationales Is Present With Respect To The Warrantless Search Of A Cellphone	13
III. Permitting A Warrantless Search Of A Smartphone, But Limiting It To Evidence Relating To The Crime Of Arrest Is Unworkable.	17

TABLE OF CONTENTS—continued

Page

IV. Cellphone Data Necessitates The Protections Of The Warrant Requirement. 20

A. Technology Has Removed Impediments To Securing A Warrant..... 22

B. A Warrant Is The Only Effective Mechanism For Managing Governmental Collection Of Cellphone Data..... 22

CONCLUSION 28

TABLE OF AUTHORITIES

Page(s)

CASES

Amnesty Int'l USA v. Clapper, 638 F.3d 118 (2d Cir. 2011) 2
Arizona v. Gant, 556 U.S. 332 (2009) 14, 15, 17
Bell v. Wolfish, 441 U.S. 520 (1979) 21
Bertot v. Sch. Dist. No. 1, Albany Cnty., Wyo., 613 F.2d 245 (10th Cir. 1979) 10
California v. Chimel, 395 U.S. 752 (1969) 11, 12, 13
Channel 10, Inc. v. Gunnarson, 337 F. Supp. 634 (D. Minn. 1972) 10
Coolidge v. New Hampshire, 403 U.S. 443 (1971) 11, 21
Dunaway v. New York, 442 U.S. 200 (1979) 26
Fed. Election Comm'n v. Wis. Right to Life, Inc., 551 U.S. 449 (2007) 10
Hepting v. AT&T Corp., 539 F.3d 1157 (9th Cir. 2008) 2
Illinois v. Caballes, 543 U.S. 405 (2005) 27
In re Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109 (N.D. Cal. 2008) 2
Jones v. United States, 357 U.S. 493 (1958) 11
Katz v. United States, 389 U.S. 347 (1967) (Harlan, J. concurring) 3
Knowles v. Iowa, 525 U.S. 113 (1998) 11
Kyllo v. United States, 533 U.S. 27 (2001) 3
McDonald v. United States, 335 U.S. 451 (1948) 11

TABLE OF AUTHORITIES—continued

Page(s)

Missouri v. McNeely, 133 S. Ct. 1552 (2013) 22
People v. Diaz, 244 P.3d 501 (Cal. 2011) 13
Roaden v. Kentucky, 413 U.S. 496 (1973) 9, 10
Robinson v. Fetterman, 378 F. Supp. 2d 534 (E.D. Pa. 2005) 10
Rossignol v. Voorhaar, 316 F.3d 516 (4th Cir. 2003) 9
Sibron v. New York, 392 U.S. 40 (1968) 15
Smith v. State, 981 N.E.2d 1262 (Ind. Ct. App. 2013), *transfer denied*, 996 N.E.2d 328 (Ind. 2013) 22
State v. Hathaway, No. A-3986-12T4, 2013 WL 6223364 (N.J. Super. Ct. App. Div. Dec. 2, 2013) 22
State v. Nordlund, 53 P.3d 520 (Wash. Ct. App. 2002) 9
State v. Zeller, 172 Wash. App. 1008 (2012) 22
United States v. Chadwick, 433 U.S. 1 (1977) 14, 15
United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993) 24
United States v. Comprehensive Drug Testing, 621 F.3d 1162 (9th Cir. 2010) 27
United States v. Finley, 477 F.3d 250 (5th Cir. 2007) 23
United States v. Hill, 459 F.3d 966 (9th Cir. 2006) 27
United States v. Jones, 132 S. Ct. 945 (2012) 2
United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996) 23

TABLE OF AUTHORITIES—continued

Page(s)

United States v. Robinson, 414 U.S. 218 (1973) 12, 23
United States v. U.S. Dist. Ct. E.D. Mich., S. Div., 407 U.S. 297 (1972) 6
United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *cert. granted*, No. 13-212 (U.S. Jan. 17, 2014) 26

COURT DOCUMENT

Pet'r's Br., *United States v. Wurie*, No. 13-212 (U.S. Mar. 3, 2014) 15, 17, 19, 23

OTHER AUTHORITIES

Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 Ariz. L. Rev. 577 (2012) 18
Amanda Lenhart, *Cellphones and American Adults* (2010) 8
App Store Metrics, 148 Apps, http://148apps.biz/app-store-metrics/ (last updated Mar. 3, 2014) 19
Associated Press, *Chicago Sun-Times Lays Off All its Full-Time Photographers*, N.Y. Times (May 31, 2013) 9
Cell Phone Investigative Kiosks, RCFL, http://www.rcfl.gov/DSP_P_CellKiosk.cfm (last visited Mar. 3, 2014) 23
Data Capacity Converter Online, Unit Converter, http://www.unitarium.com/data (last visited Mar. 7, 2014) 4

TABLE OF AUTHORITIES—continued

Page(s)

David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205 (2009) 5

Dep't of Justice, Computer Crime & Intellectual Prop. Sec., *Awareness Brief: Find My iPhone* (June 18, 2009) 16

Elec. Frontier Found., *Report on the Investigative Data Warehouse* (2009) 24

Emily Berman, *Domestic Intelligence: New Powers, New Risks* (2011) 2

Facebook, Ericsson & Qualcomm, *A Focus on Efficiency*, internet.org (2013) 7

FBI, Dep't of Justice, *Regional Computer Forensics Laboratory Program: Annual Report* (2012) 22, 23

Gary Krakow, *Smartphones, Meet the Terabyte*, The Street (Feb. 17, 2009) 4

Harris Interactive, *Mobile Mindset Survey* (2012) 8

Josh Constine, *Facebook Reveals 78% of US Users are Mobile as it Starts Sharing User Counts by Country*, Tech Crunch (Aug. 13, 2013) 8

Jumio, *Mobile Consumer Habits 2013 Study* (2013) 8

Michael Price, *National Security and Local Police* (2013) 2

Office of Dir. of Nat'l Intelligence, N1-65-10-31, *Request for Records Disposition Authority* (2010) 24

TABLE OF AUTHORITIES—continued

Page(s)

Office of Inspector Gen., Dep't of Justice, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (2007) 24

Office of Inspector Gen., Dep't of Justice, Audit Rep. No. 05-07, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project* (2005) 24

Office of Prof'l Responsibility, FBI, *OPR's Quarterly All Employee E-mail January 2011 Edition* (Washington, D.C. Jan. 2011) 25

Office of Prof'l Responsibility, FBI, *Quarterly Emails: #9 – April 2008* (Washington, D.C. Apr. 2008) 25

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) 26, 27

Pages in a MB/GB e-Discovery Calculator, Lexbe, http://www.lexbe.com/hp/Pages-Megabyte-Gigabyte.aspx (last visited Mar. 7, 2014) 4

Rachel Levinson-Waldman, Brennan Ctr. for Justice, *What the Government Does with Americans' Data* (2013) 2, 25

Radicati Grp., Inc., *Email Statistic Report, 2012-2016* (2012) 7

Susannah Fox, *51% of U.S. Adults Bank Online*, Pew Research Ctr. (2013) 7

Susannah Fox & Maeve Duggan, *Mobile Health 2012*, Pew Research Ctr. (2012) ... 7

Terabyte Capacity for Smartphones, Telecomasia.net (Feb. 16, 2009) 4

TABLE OF AUTHORITIES—continued

Page(s)

Tim Dees, *Roadside Cellphone Data Extraction* (2011) 16

U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Border Searches of Electronic Devices* (2009) 25

INTEREST OF AMICI CURIAE[1]

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense lawyers to ensure justice and due process for persons accused of crime or other misconduct. NACDL was founded in 1958.

NACDL has a nationwide membership of approximately 10,000 and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, active U.S. military defense counsel, law professors and judges. NACDL provides amicus assistance on the federal and state level in cases that present issues of importance, such as the one presented here, to criminal defendants, criminal defense lawyers, and the proper and fair administration of criminal justice.

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and limits on executive power in the fight against terrorism. The Center's Liberty and National Security (LNS) Program fights to ensure that our nation's commitment to national security respects constitutional values and the rule of law through innovative policy recommendations, litigation and public advocacy. The

---

[1] Both parties have filed blanket consent for amicus appearance in this matter. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. This brief does not purport to convey the position of NYU School of Law. It was written with the assistance of Amos Toh, Katz Fellow at the Brennan Center.

Brennan Center is particularly concerned with domestic counterterrorism policies, including the dragnet collection of Americans' communications and personal data, and their effects on privacy and First Amendment freedoms. As part of this effort, the Center has published a series of reports on how law enforcement and intelligence agencies collect, share and retain information about Americans for national security purposes. *See* Michael Price, *National Security and Local Police* (2013); Rachel Levinson-Waldman, *What the Government Does with Americans' Data* (2013); Emily Berman, *Domestic Intelligence: New Powers, New Risks* (2011). The Center has also filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008).

SUMMARY OF THE ARGUMENT

Amici encourage this Court to prohibit the warrantless search of cellphones incident to arrest. Both the technical capacity of these devices to store great volumes of information, and the deeply private manner in which smartphones have become integrated into all aspects of daily living, create a significant privacy interest in their contents.

The search incident to arrest doctrine is governed by the rationale set forth in *California v. Chimel*. *Chimel's* twin exigencies, the need to protect officer safety, and the need to secure perishable evidence, are not present in the context of phone data. Cellphone data poses no threat to officer safety, and once

the phone has been reduced to police control, any risk of data loss is negligible.

Moreover, unlike in the context of vehicle searches, limiting a search to evidence related to the crime of arrest is unworkable with respect to cellphones. The nature and quantity of data on cellphones will mean that law enforcement will always be able to draw a connection between the offense of arrest and the phone, rendering a *Gant* limit a nullity. And practically, it is impossible for an officer in the field to conduct an appropriately limited search of digital data.

ARGUMENT

I. Mobile Computing Devices Like The Modern Smartphone Are Unique.

The Fourth Amendment is not blind to the advances of modern living. What is a reasonable search under the Fourth Amendment is a function of the privacy that society attaches to the place or object searched. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring). Reasonableness is not fixed to a particular technology level, unable to move beyond footlockers and cigarette packs, leaving the citizenry at the "mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35 (2001). Rather, as technology advances, and society's use of that technology creates new privacy expectations, what is reasonable is viewed anew.

A. The Capacity Of Mobile Computing Devices Renders Analogies To Physical Containers Inapplicable.

Any smartphone is capable of storing digital information locally, meaning that the physical device is the repository of the information. It is when we are discussing localized storage that analogizing these

devices to containers is even possible. However, the volume of information stored strains that analogy.

Current models of smartphones, such as the Apple iPhone and Samsung Galaxy S4 have 64GB (gigabytes) of localized storage. And storage capacity of models continues to expand with each new iteration.

In 2009, data storage manufacturers announced the development of the next-generation data storage architecture for phones, SDXc (Secure Digital Extended Capacity). The iPad2, one of the first devices to employ SDXc, is available in a 128 GB configuration. And SDXc is expected to push iPhones and other smartphones into the area currently reserved for laptop computers: the terabyte. Smartphones with storage in the 1-2 TB range are expected within this decade.[2] To place that number in perspective, a 1 TB phone could contain 120 hours of DVD-quality video, 720 hours of audio recordings, 22,200 high-res color photographs, 6,300,000 pages of MS Word documents and 97 million emails *all at once*, and still only be three-quarters full.[3]

With SDXc as the new storage architecture standard, individuals will truly have the capacity to store

---

[2] *See* Gary Krakow, *Smartphones, Meet the Terabyte*, The Street (Feb. 17, 2009), http://www.thestreet.com/story/10464195/smartphones-meet-the-terabyte.html; *and Terabyte Capacity for Smartphones*, Telecomasia.net (Feb. 16, 2009), http://www.telecomasia.net/content/terabyte-capacity-smartphones-0.

[3] Determining digital storage capacity is simply a mathematical calculation. To aid in that calculation, Petitioner refers this Court to a number of data storage computational aids online. *See, e.g, Data Capacity Converter Online*, Unit Converter, http://www.unitarium.com/data (last visited Mar. 7, 2014); *or Pages in a MB/GB e-Discovery Calculator*, Lexbe, http://www.lexbe.com/hp/Pages-Megabyte-Gigabyte.aspx (last visited Mar. 7, 2014).

an entire lifetime's data in their pocket. Videos of one's wedding, the birth of one's children, and every family reunion and school performance will easily fit on the device. Assuming 10 one-minute voicemails a day, everyday, the phone will hold over eleven years of voicemail messages. If you took three photographs of your child everyday of his life, from birth through high-school graduation, they would all fit on the phone with room to spare. It would easily contain not just every document you authored, but every page of every document you have ever read. Finally, it would hold every email and text message you have ever received or sent – *for your entire lifetime.*

Even though the capacity of localized storage strains traditional human conceptualizations of size, it is dwarfed by a cellphone's secondary storage mechanism: cloud data.

Cloud data is not stored locally, at least not all of it. Rather, the physical device contains tags, or permanent conduits (*i.e.*, saved encrypted passwords and account numbers) to data stored outside the physical device, on distributed systems shared across the internet. As one commentator summarized:

> Experts have coined the term 'Web 2.0' to describe the shift in Internet usage from consumption to participation and metaphorically refer to this virtual platform as 'the cloud,' where users interact with Internet applications and store data on distant servers rather than on their own hard drives.

David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, 2205 (2009).

Freed from physical restrictions, cloud computing allows cellphones to achieve infinite data capacity. By distributing data storage outside the device, and using the local storage to house conduits and tags to that data, pulling it down to the device on demand, there is literally nothing that cannot be stored on a device that fits in one's pocket.

B. Mobile Devices Have Been Incorporated Into Modern Living In A Fundamentally Private And Personal Way.

The mobile computing revolution has shifted societal concepts of identity and privacy in ways unimaginable just two decades ago. This Court has viewed the home as the epicenter of Fourth Amendment privacy. *United States v. U.S. Dist. Ct. E.D. Mich., S. Div.*, 407 U.S. 297, 313 (1972). Yet the Amendment on its face offers no distinction between "persons, houses, papers and effects."

At the time of the Fourth Amendment's enactment, the home was a locus of one's private life. Money might be held in a strongbox. Documents, deeds, wills, and investments would likely be stored in one's study. A diary detailing health problems and sickness might be tucked away in a drawer while personal letters and a family portrait would sit upon one's desk. In essence, the home was where the documentary evidence of one's self identity could be found. But the digital revolution has distributed those private pieces of one's life across cyberspace.

No longer is one's money tangible, and located in a strongbox, now it is accessible through a banking app. According to the Pew Research Center at least a

third of all mobile phone users regularly use the phone to manage their finances.[4]

A diary of one's ailments is no longer in a drawer, but is more likely to be in the cloud, accessible from a health application on a mobile phone. Over half of all smartphone owners use their phones to manage their health records, or to research health-related issues. Susannah Fox & Maeve Duggan, *Mobile Health 2012*, Pew Research Ctr. (2012).[5]

While paper correspondence has become a lost art, electronic correspondence has exploded. Ninety million Americans access email over a smartphone, and over 20 billion emails are accessed over smartphones each day worldwide. Radicati Grp., Inc., *Email Statistic Report, 2012-2016* (2012).[6] And although our mantles may still hold a small number of framed pictures, the real repository of our photographs exists on our phones and online. Facebook reports that users upload 350 million photographs to the site each day.[7]

---

[4] Report available at: Susannah Fox, *51% of U.S. Adults Bank Online*, Pew Research Ctr. (2013), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Online Banking.pdf.

[5] Report available at: http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobileHealth2012_FINAL.pdf.

[6] Report available at: http://www.radicati.com/wp/wp-content/uploads/2012/04/Email-Statistics-Report-2012-2016-Executive-Summary.pdf.

[7] Report available at: Facebook, Ericsson & Qualcomm, *A Focus on Efficiency*, internet.org (2013), *available at* https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851575_520797877991079_393255490_n.pdf.

And 468 million users access those images daily on Facebook through a mobile application.[8]

Unlike virtually any other technology, mobile devices have become an extension of one's self, completely integrated into daily living. Seventy-two percent of smartphone owners keep their phone within an arm's reach at all times. Jumio, *Mobile Consumer Habits 2013 Study.*[9] Sixty-five percent of all cellphone owners actually sleep with their phone. Amanda Lenhart, *Cellphones and American Adults* 11 (2010).[10] A 2012 survey found that 58% of phone owners check their phones at least once an hour, in bed before sleep and immediately upon waking. Harris Interactive, *Mobile Mindset Survey* (2012).[11] Over 50% use their phones while driving, nearly 20% use their phones during church, and 12% continue to use their phones in the shower. Jumio, *supra*.

The mobile computing revolution has created a virtual digital life that exists alongside and parallel to a physical life. Modern society now lives in both simultaneously, with each being integral to work, family, love, and daily living. And our mobile devices are the doorways to our virtual homes.

---

[8] Report available at: Josh Constine, *Facebook Reveals 78% of US Users are Mobile as it Starts Sharing User Counts by Country*, Tech Crunch (Aug. 13, 2013), http://techcrunch.com/2013/08/13/.

[9] Report available at: Jumio, *Mobile Consumer Habits 2013 Study* (2013), http://www.jumio.com/2013/07/americans-cant-put-down-their-smartphones-even-during-sex/.

[10] Report available at: http://pewinternet.org/~/media//Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf.

[11] Report available at: Harris Interactive, *Mobile Mindset Survey* (2012), *available at* https://www.lookout.com/resources/reports/mobile-mindset.

C. The Smartphone Is The New Instrument Of First Amendment Expression.

Lower courts have noted that, by their range of capabilities, ease of access, and societal saturation, smartphones are the quintessential free speech instruments of our age:

> The trial court aptly described a personal computer as 'the modern day repository of a man's records, reflections, and conversations.' CP at 200. Thus, the search of that computer has first amendment implications that may collide with fourth amendment concerns.

State v. Nordlund, 53 P.3d 520, 525 (Wash. Ct. App. 2002) (citation omitted). Even major news media such as the Chicago Sun Times have eschewed staff photographers, and now issue their reporters smartphones.[12]

This Court has afforded heightened protection to First Amendment instruments. The warrantless search of such material is a form of prior restraint, a long disfavored practice. *Roaden v. Kentucky*, 413 U.S. 496, 503 (1973) (When an officer "br[ings] to an abrupt halt an orderly and presumptively legitimate distribution or exhibition" of material protected by the First Amendment, such action is "plainly a form of prior restraint and is, in those circumstances, unreasonable under Fourth Amendment standards."). *See also Rossignol v. Voorhaar*, 316 F.3d 516, 522 (4th Cir. 2003) (Where sheriff's deputies suppressed newspapers critical of the sheriff "before the critical

---

[12] *See* Associated Press, *Chicago Sun-Times Lays Off All its Full-Time Photographers*, N.Y. Times (May 31, 2013), http://www.nytimes.com/2013/06/01/business/media/chicago-sun-times-lays-off-all-its-full-time-photographers.html?_r=3&.

commentary ever reached the eyes of readers, their conduct met the classic definition of a prior restraint.").

In an age when anyone can use a cellphone to blog, post to newsgroups, capture still images and video, send correspondence, and use all form of social mass communication, an officer's warrantless search of such a First Amendment instrumentality must be judged according to a stricter standard. *See Robinson v. Fetterman*, 378 F. Supp. 2d 534, 541 (E.D. Pa. 2005) (By restraining an individual from "publicizing or publishing what he ha[s] filmed," officers' "conduct clearly amount[s] to an unlawful prior restraint upon his protected speech."); *Channel 10, Inc. v. Gunnarson*, 337 F. Supp. 634, 637 (D. Minn. 1972) ("[I]t is clear to this court that the seizure and holding of the camera and undeveloped film was an unlawful 'prior restraint' whether or not the film was ever reviewed."). The warrantless seizure of material protected by the First Amendment "calls for a higher hurdle in the evaluation of reasonableness" under the Fourth Amendment. *Roaden*, 413 U.S. at 504.

This Court has noted that, when faced with a close call, "the First Amendment requires [courts] to err on the side of protecting . . . speech rather than suppressing it." *Fed. Election Comm'n v. Wis. Right to Life, Inc.*, 551 U.S. 449, 457 (2007); *see also Bertot v. Sch. Dist. No. 1, Albany Cnty., Wyo.*, 613 F.2d 245, 252 (10th Cir. 1979) ("We prefer that governmental officials acting in sensitive First Amendment areas err, when they do err, on the side of protecting those interests.").

II. The Warrantless Search Of A Smartphone Incident To Arrest Is Not Justified Under The Search Incident To Arrest Doctrine.

As this Court has consistently held, "the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment.'" *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971).

Exceptions to the warrant requirement are to be jealously and carefully drawn. *Jones v. United States*, 357 U.S. 493, 499 (1958). Such exceptions cannot be based upon mere governmental desire, or even need. Rather, warrant exceptions stake a claim to the Fourth Amendment's bedrock requirement of reasonableness only by "a showing by those who seek exemption from the constitutional mandate that the exigencies of the situation made that course imperative." *McDonald v. United States*, 335 U.S. 451, 456 (1948).

The search incident to arrest doctrine, as a historical exception to the warrant requirement, becomes reasonable only when two exigencies are present: "(1) the need to disarm the suspect in order to take him into custody, and (2) the need to preserve evidence for later use at trial." *Knowles v. Iowa*, 525 U.S. 113, 116 (1998) (citing cases going back to *Weeks v. United States*, 232 U.S. 383, 392 (1914)).

This Court laid down the "proper extent" of a seizure incident to lawful arrest in *California v. Chimel*, where it invalidated the search following respondent's arrest of his "entire three bedroom house, including the attic, the garage, and a small workshop." *California v. Chimel*, 395 U.S. 752, 754 (1969). Because "'[t]he scope of [a] search must be "strictly tied

to and justified by" the circumstances which rendered its initiation permissible,'" the *Chimel* Court set forth a rule to ensure that searches incident to arrest are linked to, and do not exceed, the two exigency rationales that render them "imperative." *Id.* at 761-62. Recognizing that weapons can be used to effect an assault or escape and evidence can be destroyed or concealed only to the extent they are accessible to the arrestee, this Court held that authorities, incident to lawful, custodial arrest, may search only an arrestee's person and his area of "immediate control . . . mean[ing] the area from within which he might gain possession of a weapon or destructible evidence." *Id.* at 763 (quotation marks omitted).

This Court's decision in *Robinson* did not alter the twin exigencies of *Chimel*. In *Robinson*, this Court held that:

> It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment.

United States v. Robinson, 414 U.S. 218, 235 (1973).

Robinson simply extended the need to establish officer safety and secure evidence to a defendant's pockets. *Robinson* never purported to countenance a general rummaging of one's life upon arrest, as this Court cautioned against in *Chimel*:

> After arresting a man in his house, to rummage at will among his papers in search of whatever will convict him, appears to us to be indistinguishable from what might be done under a general warrant; indeed, the warrant would give

> more protection, for presumably it must be issued by a magistrate. True, by hypothesis the power would not exist, if the supposed offender were not found on the premises; but it is small consolation to know that one's papers are safe only so long as one is not at home.

395 U.S. at 767-68 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.))

The Supreme Court of California's decision in *People v. Diaz*, which controlled the outcome in this case, untethers *Robinson* from the *Chimel* rationale, rendering the result absurd. *People v. Diaz*, 244 P.3d 501, 505 (Cal. 2011). *Chimel* prevents a rummaging through one's home, but apparently under the government's interpretation, if technology advances sufficiently to digitize and shrink the contents of that home into one's pocket, the search becomes reasonable. The Constitution is not quantum mechanics; the rules do not break down when we move from the scale of the large to the small. *Chimel* still applies, and under *Chimel* the search is not permitted.

A. Neither Of The *Chimel* Rationales Is Present With Respect To The Warrantless Search Of A Cellphone.

Neither of the *Chimel* rationales supports the warrantless search of a cellphone incident to arrest. First, there is no officer safety concern posed by the data. Digital data is not a razor blade, or a firearm. It cannot harm, or in any way endanger, the arresting officers.

And once the phone is reduced to police custody, there is no reasonable likelihood of the destruction of evidence. Once the phone is in police control, the data is secure, just as the footlocker was secure in *United*

States v. Chadwick, where this Court struck down a search occurring 90 minutes after arrest. This Court reasoned that a search is not "incident to th[e] arrest either if the search is remote in time or place from the arrest or no exigency exists" and that authorities had removed the footlocker to "their exclusive control" before searching it, so "there [was] no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence." *United States v. Chadwick*, 433 U.S. 1, 15 (1977).

This Court reiterated the *Chimel/Chadwick* line of reasoning again in *Gant*, holding that the search incident to arrest of a vehicle already reduced to exclusive police control is not reasonable:

> In *Chimel*, we held that a search incident to arrest may only include 'the arrestee's person and the area 'within his immediate control' – construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.' *Ibid.* That limitation, which continues to define the boundaries of the exception, ensures that the scope of a search incident to arrest is commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy . . . If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply.

Arizona v. Gant, 556 U.S. 332, 339 (2009) (quoting *Chimel*, 395 U.S. at 763).

Respondent may argue, as does the Solicitor General in *United States v. Wurie*, that law enforcement

risks the data being "wiped" remotely. Pet'r's Br. 37-39, *United States v. Wurie*, No. 13-212 (U.S. Mar. 3, 2014). But that argument rings hollow. At the outset, this Court should note that the government offers no concrete example of that risk materializing. As Justice Scalia noted in the context of vehicle searches "the government . . . failed to provide a single instance in which a formerly restrained arrestee escaped to retrieve a weapon from his own vehicle." *Gant*, 556 U.S. at 352 (Scalia, J., concurring). The same holds true here. If remote data loss is a real threat to evidence the government should be able to provide this Court examples of cases in which data was lost during the time between seizure of a phone and the "hours or minutes necessary to obtain a warrant." *Chadwick*, 433 U.S. at 13.

Even if such case examples do exist, the objectively reasonable likelihood of data loss must be evaluated in reference to "the concrete factual context of the individual case." *Sibron v. New York*, 392 U.S. 40, 59 (1968). It would be a rare case indeed, one involving a well-coordinated conspiracy of highly technically sophisticated suspects, where a threat of data wiping is even plausibly objectively reasonable. It certainly is not reasonable in respect to the vast majority of arrests for crimes such as DUI, assault, burglary, et cetera.

Moreover, in those very unusual cases where data wiping could even potentially occur, law enforcement has multiple ways to prevent the possibility from materializing.

First, law enforcement agencies throughout the country already employ portable devices, such as the CelleBrite UFED, designed to copy the entire data contents of a cellphone within minutes in the field.

Law enforcement proponents have praised the ease of use of the UFED device:

> Operation of the UFED is very straightforward. The investigator first needs to know the brand and model of the phone to be examined. More than 1,800 models are supported, and the list is updated at least once per month. Checking an index of supported models will indicate the data cable the investigator needs to use from the 80 supplied with the device. Connect the phone to the UFED using the appropriate cable (it's also possible to get the data via Bluetooth or IR port with some phones, but the data cable is the preferred method), tell the UFED what model phone it's examining, check the boxes alongside the types of information (phonebook, text messages, dialed numbers, photos, videos, etc.) to be retrieved, and press 'OK.'
>
> The entire process takes only a few minutes.

Tim Dees, *Roadside Cellphone Data Extraction* (2011).[13]

Second, law enforcement can employ a Faraday bag to shield a phone from data signals. This simple zip lock-style bag is made from the same material that prevents microwave ovens from spilling radiation into a kitchen. Shielded bags are widely available to law enforcement and the general public, and may be obtained from major retailers like Amazon at a minimal price point. *See, e.g.*, Dep't of Justice, Computer Crime & Intellectual Prop. Sec., *Awareness Brief: Find My iPhone* (June 18, 2009).

---

[13] Article available at: http://www.policeone.com/police-products/police-technology/mobile-data/articles/3592671-Roadside-cell-phone-data-extraction/.

Finally, if law enforcement is concerned about remote data wiping, it can employ the entirely effective and cost free solution of simply powering the phone off.[14]

III. Permitting A Warrantless Search Of A Smartphone, But Limiting It To Evidence Relating To The Crime Of Arrest Is Unworkable.

In *Gant*, this Court permitted the search incident to arrest of a vehicle when "it is reasonable to believe the vehicle contains evidence of the offense of arrest." *Gant*, 556 U.S. at 351. Echoing the Solicitor General's argument in *United States v. Wurie*, Respondent may ask this Court to graft that vehicle-specific rule onto the context of cellphones. *See* Pet'r's Br. 46-48, *Wurie*, No. 13-212. This Court should decline the invitation.

First, although the government may offer *Gant* as a practical limitation, in fact it is no limit at all in this context. Because of the quantity and scope of private information available on modern cellphones, and the myriad of ways we use those phones throughout our lives, an officer justifying a search after the fact in a suppression hearing will virtually always be able to draw a plausible connection between the crime and the data.

Take for example the routine DUI stop – a crime typically not requiring evidence beyond the observation of driving and a breath or blood test. Law en-

---

[14] Amici note that all of these options are themselves seizures of the phone and its data. And those seizures themselves carry constitutional implications. Amici's suggestion that UFED may obviate the need for a warrantless search should not be read as an endorsement that data copying by law enforcement is always a constitutionally permissible seizure of data.

forcement could theorize that a phone could contain pictures of the suspect drinking at the bar, text messages containing admissions of intoxication, digital receipts for the drinks ordered, and health records showing that the subject was on medication that interacted with alcohol.

A person texting while driving would have a connection between an arrestable traffic offense and their phone. Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 Ariz. L. Rev. 577, 579-80 (2012).

Low level possession of marijuana would support a phone search because the officer would only have to testify that many drug purchases are facilitated by text message. Similarly, every prostitution arrest would support the search of a phone, because perhaps the prostitute and patron coordinated via text message.

Indeed it is difficult to imagine a crime with respect to which law enforcement will not be able to say that in the officer's training and experience people tend to document their activities and leave digital records. The officer will only need to speculate about texts to potential undiscovered co-conspirators, possible photos showing the suspect with contraband, a GPS location near a crime scene, or web search history showing criminal planning to connect the phone to the crime of arrest and leverage that connection into a search of the data.

Further, the practical application of such a rule in the field is impossible. It is easy to define the acceptable parameters of a vehicle search. Objects can reasonably be located in certain places, and not in others. One need not look in the glovebox for a stolen

television. But how is an officer in the field supposed to know where in the phone to search for only the data connected to the crime of arrest?

Looking just to the online Apple application store, there are over one million unique applications available for mobile phone users, and over 1,000 new applications are added every day.[15] Existing applications are continually updated and modified, with new versions continually changing the interface and capabilities of the app. Many of the apps for mobile phones serve multiple purposes, making the type of data the app would hold difficult to determine. Applications like Snapchat mix photography with messaging. Applications like Health4Me combine messaging features with calendar appointment tracking and access to private prescription information.

This problem is further compounded by the fact that data is not cleanly divided into local data contained solely on the phone itself, versus distributed data located in the cloud. One cannot easily determine from an application where the data resides. And many applications blend local and cloud data in constructing what is displayed to the cellphone user.

The complexity and continually evolving nature of mobile data does not lend itself to ad hoc determinations made by individual law enforcement officers in the field. A *Gant* rule, or a rule that data located on the phone is searchable but distributed data is not, cannot be practically applied. *See* Pet'r's Br. 43-44, *Wurie*, No. 13-212 (arguing that a warrantless search is permissible as to local data, but conceding that such a search is impermissible as to distributed data).

---

[15] Statistics available at: *App Store Metrics*, 148 Apps, http://148apps.biz/app-store-metrics/ (last updated Mar. 3, 2014).

Imparting such rules to the cellphone context would mean requiring law enforcement officers in the field to know how each of those applications is used, which are financial applications, which hold photographs versus text, which might link to external data on the cloud, et cetera.

It would force law enforcement agents to become technology experts, knowing the latest models of devices and applications. And it would require law enforcement to become "technology sociologists," knowledgeable in the ways consumers are using the latest apps, how apps might disguise themselves as something else, or be renamed.

In short, *Gant* and other ad hoc solutions are not viable alternatives to unfettered searches in this context. The rule would simply amount to a *de facto* ratification of an exploratory search of the intimate details of an arrestee's digital life incident to arrest for any crime. It would be entirely unworkable in the field – save as a license to conduct broad and general searches of materials for which expectations of privacy are at their height. And finally, it would result in voluminous litigation. In nearly every case involving a cellphone search the defendant would demand a hearing on the officer's reasonable belief, what specific apps were searched, how the search was conducted, and how the officer chose certain data files over others. In many cases, expert testimony might be required to adequately assess the officer's explanation, and "battles of the experts" could proliferate.

IV. Cellphone Data Necessitates The Protections Of The Warrant Requirement.

The touchstone of the Fourth Amendment has always been reasonableness:

> The test of reasonableness under the Fourth

> Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted.

Bell v. Wolfish, 441 U.S. 520, 559 (1979).

The Fourth Amendment prefers warrants because warrants guarantee detached objective reasonableness in ways that warrant exceptions cannot. As this Court has said:

> 'The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers. . . . When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.'

Coolidge, 403 U.S. at 449-50.

A. Technology Has Removed Impediments To Securing A Warrant.

As this Court has noted recently, advances in technology have significantly improved the ease and speed with which law enforcement can secure a warrant. *Missouri v. McNeely*, 133 S. Ct. 1552, 1562, (2013). Applications for warrants via telephone or email are permitted under the Federal Rules of Criminal Procedure, as well as the vast majority of states.

While the time to obtain a warrant is situation-specific, courts routinely report telephonic or email warrants being secured within minutes, or the length of a typical traffic stop. *See, e.g., Smith v. State*, 981 N.E.2d 1262, 1273 (Ind. Ct. App. 2013), *transfer denied*, 996 N.E.2d 328 (Ind. 2013) (warrant obtained during traffic stop); *State v. Zeller*, 172 Wash. App. 1008 (2012) (same); *State v. Hathaway*, No. A-3986-12T4, 2013 WL 6223364 (N.J. Super. Ct. App. Div. Dec. 2, 2013) (warrant obtained in 30 minutes).

B. A Warrant Is The Only Effective Mechanism For Managing Governmental Collection Of Cellphone Data.

This case is but one example of a widespread phenomenon. Law enforcement nationwide is systematically capturing, copying, and keeping vast amounts of data from arrestees all without a warrant.

In this case, the San Diego Police Department "downloaded" videos "along with a bunch of photos" from Riley's cellphone "through RCFL." J.A. 14. "RCFL" appears to refer to San Diego's Regional Computer Forensics Laboratory, established by the FBI in partnership with local law enforcement agencies in 1999. FBI, Dep't of Justice, *Regional Computer Forensics Laboratory Program: Annual Report* 46 (2012). The FBI now operates similar partnerships

with law enforcement in nineteen states, providing local officers with assistance duplicating, storing and preserving digital evidence. The FBI provides local police with access to "Cell Phone Investigative Kiosks," which allow officers to "extract data from a cell phone, put it into a report, and burn the report to a CD or DVD in as little as 30 minutes." *Cell Phone Investigative Kiosks*, RCFL, http://www.rcfl.gov/DSP_P_CellKiosk.cfm (last visited Mar. 3, 2014). In 2012 alone, the San Diego Police Department and other law enforcement agencies in the area used the kiosks 1,575 times to extract, copy, and retain cellphone evidence. FBI, *supra*, at 46. The kiosks are becoming increasingly popular with law enforcement nationwide. In 2012, law enforcement used the kiosks 8,795 times, a 48% increase from 2011. *Id.* at 6.

A predictable consequence of warrantless cellphone searches is that at least some of the information will eventually wind up stored in a government database. If police officers do not need a warrant to search a cellphone incident to arrest – if a personal electronic device is a mere "closed container" subject to full inspection – then police will surely claim the authority to conduct an unlimited search and use the information in any way they see fit. *See* Pet'r's Br. 12-13, *Wurie*, No. 13-212 (government arguing that *"any* warrantless search of items found on the person of an arrestee" is a "reasonable search" under *Robinson*, 414 U.S. 218 (emphasis added)); *United States v. Finley*, 477 F.3d 250, 260 (5th Cir. 2007) (determining that a cellphone is a "closed container" and therefore subject to a full search incident to arrest without any additional justification); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (permitting police to search the memory of pager incident to arrest under the "closed container" rule); *United States v. Chan*,

830 F. Supp. 531, 535 (N.D. Cal. 1993) (same). Absent a warrant requirement, police may consider themselves free to create a "mirror" copy of the data, retain it on a law enforcement database for detailed analysis, and share it with other law enforcement agencies as a matter of routine.

This is not idle speculation. Although the San Diego Police Department does not publish its procedures for handling digital evidence, the FBI's rules provide a glimpse into how law enforcement retains and shares electronic data belonging to thousands of Americans. At present, all telephone data collected during FBI investigations – including data extracted from cellphones seized incident to arrest – is stored in the FBI's Telephone Applications Database. That information feeds into the Investigative Data Warehouse (IDW), a central repository completed in 2005 for criminal and counterterrorism purposes. Office of Inspector Gen., Dep't of Justice, Audit Rep. No. 05-07, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project* (2005); Elec. Frontier Found., *Report on the Investigative Data Warehouse* § II (2009). At least 12,000 federal, state and local law enforcement and government officials have access to the IDW database. Office of Inspector Gen., Dep't of Justice, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 30 n.64 (2007). There are few limits on how long the FBI can keep data in the IDW. Bureau policy states that the data is deleted or destroyed only "when superseded by updated information or when no longer needed for analytical purposes." Office of Dir. of Nat'l Intelligence, N1-65-10-31, *Request for Records Disposition Authority* (2010).

Similarly, customs officials assert broad latitude to search and copy electronic devices at the border with-

out suspicion of criminal activity. U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Border Searches of Electronic Devices* 3 (2009).[16] Officials routinely copy the contents of cellphones, cameras, and computers without any suspicion of criminal activity and keep the data if required for any "law enforcement purpose." *Id.* at 3. The Department of Homeland Security (DHS) then retains this information on a variety of databases for 5, 15, or 20 years, and may use or share it broadly to assist in national security and intelligence activities. Levinson-Waldman, *supra*, 37, 72 nn.320-21.

Such open-ended policies raise troubling questions about the constitutionality of copying, retaining, and sharing cellphone data without limit. Can police seize every bit of data on a phone, or only the relevant data? Will the plain view doctrine apply? How long can law enforcement keep the data it copies? Should there be a requirement to purge irrelevant information? Who else can see the data and for what purpose? Can the Internal Revenue Service take a look? The lack of appropriate safeguards creates a temptation to use the data for improper reasons. For example, the FBI's Office of Professional Responsibility recently reported that FBI employees had conducted more than 1,500 unauthorized searches on FBI and government databases to look up friends working as exotic dancers and celebrities they "thought were hot." Office of Prof'l Responsibility, FBI, *OPR's Quarterly All Employee E-mail January 2011 Edition*, at § 9 (Washington, D.C. Jan. 2011); Office of Prof'l Responsibility, FBI, *Quarterly Emails: #9 – April 2008*,

---

[16] Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

at § 14 (Washington, D.C. Apr. 2008).[17] A warrant requirement will not make these questions disappear, but it will ensure that troves of highly personal data do not wind up on a government computer network without adequate justification. Courts can craft reasonable parameters for the search that are consistent with the particularity requirement of the Fourth Amendment, minimize the invasion of privacy, and prevent personal data from being copied needlessly, kept indefinitely, or used improperly.

A bright line warrant requirement will also alleviate uncertainty for police officers in the field, placing questions regarding the scope of the search under *ex ante* judicial supervision. There may be a temptation to craft a graduated approach to cellphone searches; to require a warrant for copying the contents, but not to browse through a few screens, for example. But such an approach would force law enforcement officers with "only limited time and expertise" and in the heat of an investigation to "reflect on and balance the social and individual interests in the specific circumstances they confront." *Dunaway v. New York*, 442 U.S. 200, 214 (1979); *United States v. Wurie*, 728 F.3d 1, 6 (1st Cir. 2013), *cert. granted*, No. 13-212 (U.S. Jan. 17, 2014).

Absent a warrant requirement, there is simply no clear way to regulate the scope of the intrusion. Even the most cursory search – for example, a search for a particular name or number – can transform into an extensive forensic search that yields large volumes of private and sensitive information. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 565-66, 569 (2005). Moreover, there

---

[17] Available at: http://i2.cdn.turner.com/cnn/2011/images/01/27/fbi.documents.siu.pdf.

would be no mechanism to regulate how long police can keep cellphone data or control who has access to it. This Court has recognized that even an initially permissible seizure can become unreasonable "if it is prolonged beyond the time reasonably required to complete th[e] mission." *Illinois v. Caballes*, 543 U.S. 405, 407 (2005). But if there is no "mission" – if the only justification for seizing and searching cellphone data is that it occurs incident to arrest – then the scope of the intrusion is limited only by the officers' time and imagination. *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1171 (9th Cir. 2010) (observing that without judicially imposed limits on the scope of digital searches, "government agents ultimately decide how much to actually take . . . creat[ing] a powerful incentive for them to seize more rather than less"); Kerr, *supra*, at 544. Every police department in the country could have a different rule about what data to keep and share.

A neutral and detached magistrate is well placed to weigh the Fourth Amendment considerations in the balance and ensure meaningful limits on the scope of cellphone searches. *Comprehensive Drug Testing*, 621 F.3d at 1179 (Kozinski, J., concurring) (observing that magistrate judges can require the government to waive reliance on the plain view doctrine, segregate relevant evidence from unrelated data and return or destroy unrelated data). In some instances, there may be good reason to copy phone data or to conduct a forensic analysis, but that reason should be presented to a court before the government can "seize the haystack to look for the needle." *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006).

CONCLUSION

For the foregoing reasons, amici urge this Court to reverse the decision of the California Supreme Court and hold that the search incident to arrest doctrine does not justify the search of the data contents of a cellphone.

Respectfully submitted,

JEFFREY T. GREEN
CO-CHAIR, AMICUS COMMITTEE
NAT'L ASS'N OF CRIMINAL DEFENSE LAWYERS
1501 K Street, N.W.
Washington, D.C. 20005

BRONSON D. JAMES*
BRONSON JAMES LLC
522 N.W. 23rd Ave.
Portland, OR 97210
(503) 943-6876
bj@bronsonjames.com

MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
161 Ave. of the Americas,
New York, NY 10013

Counsel for Amici Curiae

March 10, 2014

* Counsel of Record

AMICUS CURIAE BRIEF

RECORD AND BRIEFS

FILED
MAR 10 2014
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 13-132 and No. 13-212

IN THE
Supreme Court of the United States

DAVID LEON RILEY,
Petitioner,
v.
STATE OF CALIFORNIA,
Respondent.

On Writ of Certiorari to the California Court of Appeal, Fourth District

UNITED STATES,
Petitioner,
v.
BRIMA WURIE,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the First Circuit

BRIEF *AMICI CURIAE* OF NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION AND THIRTEEN MEDIA ORGANIZATIONS IN SUPPORT OF PETITIONER RILEY AND RESPONDENT WURIE

Thomas R. Burke
Davis Wright Tremaine LLP
505 Montgomery Street
Ste. 800
San Francisco, CA 94111
(415) 276-6500

Robert Corn-Revere*
Ronald G. London
Lisa B. Zycherman
Davis Wright Tremaine LLP
1919 Pennsylvania Ave., NW, Ste. 800
Washington, DC 20006
(202) 973-4200
bobcornrevere@dwt.com

Counsel for *Amici Curiae* *Counsel of Record

LEGAL PRINTERS LLC, Washington DC • 202-747-2400 • legalprinters.com

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF *AMICI CURIAE* 1

BACKGROUND 2

SUMMARY OF ARGUMENT 5

ARGUMENT 7

I. WARRANTLESS SEARCHES OF CELL PHONES THREATEN TO UNDERMINE THE INTERRELATED RIGHTS OF FREEDOM FROM UNREASONABLE SEARCHES, FREE EXPRESSION, AND FREEDOM FROM SELF-INCRIMINATION 7

A. Cell Phones Are Essential Tools of Self-Expression and Modern Journalism 7

B. Fourth Amendment Analysis Must Take Into Account Changes in Technology 14

C. Fourth Amendment Protections Also Implicate First and Fifth Amendment Rights 19

II. THIS COURT MUST MAKE CLEAR THAT SEARCH OF A CELL OR SMART PHONE REQUIRES A WARRANT 23

CONCLUSION 26

APPENDIX A
Descriptions of *Amici* 1a

APPENDIX B
List of Additional Counsel 6a

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Boyd v. United States,
116 U.S. 616 (1886) 20, 21

Garcia v. Montgomery County Police,
No. 8:12-cv-03592-JFM (D. Md.) 13

Glik v. Cunniffe,
655 F.3d 78 (1st Cir. 2011) 12

Ex Parte Jackson,
96 U.S. 727 (1877) 21, 22

Katz v. United States,
389 U.S. 347 (1967) 17

Kyllo v. United States,
533 U.S. 27 (2001) 14, 15

Marcus v. Search Warrant,
367 U.S. 717 (1961) 6, 19, 21, 25

Olmstead v. United States,
277 U.S. 438 (1928) 15, 16, 24, 25

Roaden v. Kentucky,
413 U.S. 496 (1973) 22, 23

Sharp v. Baltimore City Police,
No. 1:11-cv-02888-CCB (D. Md.) 12, 13

Talley v. California,
362 U.S. 60 (1960) 20

United States v. Flores-Lopez,
670 F.3d 803 (7th Cir. 2012) 24

United States v. Jones,
132 S. Ct. 945 (2012) 6, 15, 17, 23

United States v. Wurie,
728 F.3d 1 (1st Cir. 2013) ..... *passim*

State Cases

People v. Diaz,
51 Cal. 4th 84 (2011) 5, 23

People v. Riley,
2013 WL 475242 (Cal. App. 4th
Feb. 8, 2013) 23

Constitutional Provisions

U.S. Const. amend. I ..... *passim*

U.S. Const. amend. IV ..... *passim*

U.S. Const. amend. V 6, 19, 23, 25

Statutes

42 U.S.C. § 20000aa(b) 10

Other Authorities

Alan Pell Crawford, Founding Fathers'
Forum, Wall St. J., Feb. 2, 1995 20

At Occupy protests, U.S. journalists arrested, assaulted, Nov. 11, 2011, http://www.cpj.org/blog/2011/11/at-occupy-protests-us-journalists-arrested-assault.php 11

Charges dropped against photographers arrested in Idaho and New Mexico, Sept. 25, 1995, http://www.rcfp.org/browse-media-law-resources/news/charges-dropped-against-photographers-arrested-idaho-and-new-mexico 9

David Becker, Detroit Newspaper Photographer Arrested While Covering Police Action, July 16, 2013, http://petapixel.com/2013/07/16/detroit-newspaper-photographer-arrested-while-covering-police-action/ 11

Erin F. Fonté, Overview of Mobile Payments in the United States, 32 Banking & Financial Services Policy Report No. 8 (Aug. 2013) 18

Gary Marshall and Kate Solomon, Apple iWatch release date, news and rumors, http://www.techradar.com/us/news/portable-devices/apple-iwatch-release-date-news-and-rumours-1131043 (last visited Mar. 6, 2014) 18

Georgia newspaper chain closes its photo department, tells reporters to take pictures, July 12, 2013, http://jimromenesko.com/2013/07/12/georgia-newspaper-chain-closes-its-photo-department-tells-reporters-to-take-pictures/ 8

Google Glass, Google+, https://plus.google.com/+GoogleGlass/posts (last visited Mar. 6, 2014) 18

Henry K. Lee, UC pays to settle photographer's suit over arrest, July 2, 2012, http://www.sfgate.com/bayarea/article/UC-pays-to-settle-photographers-suit-over-arrest-3679859.php 9

Jim Schaefer, No charges for Detroit Free Press photographer or police officer after cell-phone seizure and arrest, Aug. 24, 2013, http://www.freep.com/article/20130823/NEWS01/308230111/detroit/free/press-photographer-mandi-wright-officer-Lamar-Penn 11

Josh Stearns, Citizen Journalist Arrests on the Rise at Occupy Protests, Jan. 10, 2012, http://www.freepress.net/blog/12/01/10/citizen-journalist-arrests-rise-occupy 11

Josh Stearns, Tracking Journalist Arrests at Occupy Protests Around the Country, http://storify.com/jcstearns/tracking-journalist-arrests-during-the-occupy-prot (last visited Mar. 6, 2014) 11

Mark Seagraves, Journalists won't face charges, June 24, 2011, http://www.wjla.com/articles/2011/06/journalists-won-t-face-charges-62814.html 9, 10

Mayor apologizes to photographer for arrest at football game, Aug. 24, 1998, http://www.rcfp.org/browse-media-law-resources/news/mayor-apologizes-photographer-arrest-football-game 9

Memoto Lifelogging Camera, Memoto, https://www.kickstarter.com/projects/martinkallstrom/memoto-lifelogging-camera (last visited Mar. 6, 2014) 18

Photographers arrested during rioting, imprisoned overnight, Aug. 24, 1998, http://www.rcfp.org/browse-media-law-resources/news/photographers-arrested-during-rioting-imprisoned-overnight 8, 9

Police launch investigation after wrongful arrest of editor, photographer, Aug. 14, 1985, http://www.rcfp.org/browse-media-law-resources/news/police-launch-investigation-after-wrongful-arrest-editor-photographe.....9

Sarah Rafsky, Protest Puts Coverage in Spotlight, N.Y. Times, Nov. 21, 2011, available at 2011 WLNR 24091906.....11

Shane Bowman and Chris Willis, "We Media: How Audiences are Shaping the Future of News and Information," July 2003, The Media Center at the American Press Institute, available at http://www.mediacenter/org/mediacenter/research/wemedia/ 12

Steve Myers, News photographer arrested on Long Island for videotaping police, Aug. 2, 2011, http://www.poynter.org/latest-news/mediawire/141291/news-photographer-arrested-on-long-island-for-videotaping-police/ 8, 9

Tim Worstall, This Might Not Work: Chicago Sun Times Fires All Its Photographers To Replace Them With iPhones, June 3, 2013, http://www.forbes.com/site/timworstall/2013/06/03/this-might-not-work-chicago-sun-times-fires-all-its-photographers-to-replace-them-with-iphones/ 8

Times Photographer Is Arrested on Assignment, N.Y. Times, Aug. 5, 2012, available at 2012 WLNR 16502285 9

Tom Sherwood, Journalists Handcuffed, Removed From Taxi Commission Meeting, June 23, 2011, http://www.nbcwashington.com/news/politics/Journalists-Handcuffed-Removed-From-Taxi-Commission-Meeting-124384719.html 9

Wills Citty, NYPD Officer Indicted After Investigation of NPPA Member's Unlawful Arrest, Aug. 28, 2013, http://blogs.nppa.org/advocacy/2013/08/28/nypd-officer-indicted-after-investigation-of-nppa-members-unlawful-arrest/ 8

INTEREST OF *AMICI CURIAE*[1]

Much is at stake in this Court's review of whether the Fourth Amendment permits police officers to search the digital contents of an arrestee's cell phone incident to arrest. The warrantless search of a cell phone affects not only an individual's rights under the Fourth Amendment, but necessarily implicates First and Fifth Amendment rights as well. These intertwined constitutional protections are of particular concern to *Amici* – news organizations whose members use modern technology to record, document, and report events. Because of the many ways that journalists and others use cell phone technology, these cases go the heart of the concerns that led the Constitution's Framers to adopt not only the Fourth Amendment, but also protections for freedom of expression and against self-incrimination.

Amici's members use new communications technologies, including smart phones, as an integral part of their journalistic endeavors. Coverage of breaking news frequently involves contact with police, and journalists have been threatened, arrested, and sometimes charged for doing nothing more than engaging in newsgathering activities. The same has happened to private individuals who use cell phones to record and document newsworthy

---

[1]All parties have consented to this *amici curiae* brief and letters of consent have been filed with the Clerk. No counsel for a party authored this brief in whole or in part, and no person or entity other than *amici* and their counsel made a monetary contribution to the preparation or submission of this brief.

events, as advanced technology has made citizen reporting more ubiquitous.

Amici, as described in Appendix A, are fourteen of the nation's leading news organizations, including The National Press Photographers Association, The Reporters Committee for Freedom of the Press, Advance Publications, Inc., the American Society of Media Photographers, the American Society of News Editors, the Association of Alternative News Media, The E.W. Scripps Company, the Investigative Reporting Workshop at American University, The Media Consortium, the Media Law Resource Center, The New York Times Company, the Newspaper Association of America, the Online News Association, and the Student Press Law Center. *Amici's* interest in these cases is to ensure that the crucial role that journalists, members of the press, and citizen reporters play in promoting discussion of matters of public concern is not diminished.

BACKGROUND

These cases involve criminal convictions secured with the help of information obtained from defendants' cellular phones, the contents of which were searched incident to their respective arrests. In neither *Riley* nor *Wurie* were warrants secured or any other step taken to treat the phones differently from any other personal property collected in the course of effectuating arrests.

1. When a traffic-stop inventory search of Riley's car revealed firearms under the hood, Riley was arrested. Riley Pet. Br. 4. Upon his arrest, the police seized his cell phone. The phone was a touch-

screen device that could store voice and text messages, as well as photos and video, and could be used to access the Internet, among other functions.

Police made two separate warrantless searches of the phone. At the scene of the arrest, an officer scrolled through its contents – including the contact list and text messages – and found initials suggesting street-gang association. Hours later at a police station, a detective searched "a lot of stuff" on the phone "looking for evidence," Riley JA 11, 20, and found photos and videos also suggestive of gang affiliation.

Based on this and other evidence, Riley and two others were charged with various offenses, including an allegation that their crimes were gang-related. Riley moved to suppress all evidence obtained during the searches of his cell phone, arguing they violated the Fourth Amendment given the absence of a warrant or any exigency justifying a search. *Id.* 269-70. The court denied the motion on grounds the phone searches were permissible incident to arrest. Riley Br. 7.

Riley's initial trial ended in a hung jury, but on retrial, the State relied on circumstantial evidence, including a photo and video gathered from the cell phone search. Riley was convicted and sentenced to a term of 15 years to life.

2. Wurie was seen by police making from his car an apparent drug sale that the officers believed had been arranged by cell phone. App. 2a, 56a. Officers following Wurie arrested him for drug distribution, brought him to a police station, and seized from him

two cell phones, along with other personal property. *Id.* at 2a, 57a.

Officers noticed that one of the cell phones, a "flip" model that must be opened to make calls, kept receiving calls from a number identified on the phone's external screen as "my house." *Id.* 2a. Officers opened the phone to view its call log, *id.* 2a-3a, and saw a photo of a woman holding a baby, *id.* 3a, then used the phone's navigation buttons to access the call log and obtain the number for "my house." *Id.* The police learned via an online directory that the phone number for "my house" corresponded to an address near where Wurie had parked before his arrest. App. 3a. Officers went to the address, identified a mailbox with Wurie's name, and through the window saw a woman resembling the photo on his phone. App. 3a-4a. Police obtained a search warrant for the premises, and there found cash, drugs, drug paraphernalia, a firearm, and ammunition. *Id.* 4a.

Wurie was charged based on evidence collected from his phone and the apartment, and the district court denied his motion to suppress. The jury convicted him, and Wurie was sentenced to over 20 years in prison.

3. Despite the commonality of Riley's and Wurie's respective convictions and sentences being supported by evidence obtained through warrantless searches of their cell phones, the decisions on review reached opposite conclusions regarding the constitutionality of the searches. In *Riley*, the California Court of Appeal affirmed the conviction, holding the cell phone searches were permissible incident to arrest,

because Riley's cell phone was "immediately associated with [his] person" at the time of arrest. Pet. App. 15a. In doing so, it relied on a California Supreme Court decision, *People v. Diaz*, 51 Cal. 4th 84 (2011), which held such cell phone searches are permissible regardless of whether an exigency for the search exists. Pet. App. 15a. The California Supreme Court denied without comment Riley's petition for discretionary review. *Id.* 24a.

In *Wurie*, the U.S. Court of Appeals for the First Circuit reversed the conviction and remanded for further proceedings. 728 F.3d at 1, 14. It held that warrantless searches of data on cell phones seized from arrestees as part of an arrest categorically exceed the bounds of the Fourth Amendment search-incident-to-arrest exception. *Id.* at 1, 12. This is so, the court reasoned, because the government failed to demonstrate that such searches are ever necessary to promote officer safety or prevent the destruction of evidence, the two bases on which the exception rests. *Id.* at 5-6, 9, 12.

Although the cases were not formally consolidated, the questions they present involve issues of surpassing importance that will determine the future robustness of numerous constitutional protections.

SUMMARY OF ARGUMENT

Neither Riley nor Wurie are reporters, nor were they using their cell phones as tools to facilitate reporting information to the public. But the fact that they were convicted based in part on words and images stored in personal electronic devices

implicates the fundamental purposes underlying not just the Fourth Amendment, but the First and Fifth Amendments as well.

Fourth Amendment analysis must account for technological change, as this Court has endeavored to ensure that "[w]hatever new methods of investigation may be devised, our task, *at a minimum*, is to decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment." *United States v. Jones*, 132 S. Ct. 945, 951 n.3 (2012). The Constitution's Framers also understood that "the unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961).

The Framers adopted strong protections against searches or seizures of persons, houses, papers, and effects so that the government could not engage in fishing expeditions to find seditious writings that could be used to incriminate citizens and thereby stifle free expression. These fundamental rights are vital for all citizens, including the defendants in these cases. But they have particular importance for photographers, journalists, and others who regularly use modern communications technologies to gather and report the news. Allowing warrantless searches of cell phones would have a particularly adverse impact on the press.

It is essential for the Court to make clear that a search warrant is required in cases like these to prevent changing technology from eroding our most basic rights.

ARGUMENT

I. WARRANTLESS SEARCHES OF CELL PHONES THREATEN TO UNDERMINE THE INTERRELATED RIGHTS OF FREEDOM FROM UNREASONABLE SEARCHES, FREE EXPRESSION, AND FREEDOM FROM SELF-INCRIMINATION

A. Cell Phones Are Essential Tools of Self-Expression and Modern Journalism

Smart phones have become an integral part of modern newsgathering technology. A typical journalist's phone contains a wealth of private data, which can include a list of personal and professional contacts, people recently called (including news sources), text messages, email, GPS location data, web browsing history, passwords, and the contents of social media accounts. In addition, journalists use smart phones to take photographs, record video, record audio, and maintain reporting notes. Thus, at any time a journalist's phone may include drafts of stories, interviews, corresponding photos or video, information about sources, and other confidential information necessary for reporting.

Of particular concern to *Amici*, media outlets increasingly rely on issuing reporters smart phones to take photographs and to record other story elements. Cell phone cameras are capable of taking high quality photographs and audio-visual recordings. And, because smart phones can connect to the Internet, it is easy for journalists to upload

photo, video, audio, or text files to the Internet to file reports. Unfortunately, the availability of smart phone photographic technology also has led to the loss of staff positions by long-time photojournalists from newspapers and television stations.[2] But whatever else this may say about the current state of the news business, the increased reliance by media organizations on such technology only heightens the importance of the issues raised by these cases.

These new technologies have greatly expanded the ability to gather and report news, but the same capabilities that make them a boon to journalists create a grave threat if they are subject to unrestricted warrantless searches incident to arrest. Unfortunately, the threat is not just hypothetical, and the enhanced newsgathering capacity may have made reporters more frequent targets of police action. There has been an epidemic of arrests for nothing more than the journalistic enterprise of photographing public events.[3] Frequently, such

---

[2] *See, e.g.*, Tim Worstall, This Might Not Work: Chicago Sun Times Fires All Its Photographers To Replace Them With iPhones, Forbes, June 3, 2013, http://www.forbes.com/sites/timworstall/2013/06/03/this-might-not-work-chicago-sun-times-fires-all-its-photographers-to-replace-them-with-iphones/; Georgia newspaper chain closes its photo department, tells reporters to take pictures, July 12, 2013, http://jimromenesko.com/2013/07/12/georgia-newspaper-chain-closes-its-photo-department-tells-reporters-to-take-pictures/.

[3] *See, e.g.*, Wills Citty, NYPD Officer Indicted After Investigation of NPPA Member's Unlawful Arrest, Aug. 28, 2013, http://blogs.nppa.org/advocacy/2013/08/28/nypd-officer-indicted-after-investigation-of-nppa-members-unlawful-arrest/; Steve Myers, News photographer arrested on Long Island for

arrests are made on generalized charges of "disorderly conduct" or "disturbing the peace," and often charges are dismissed without further action. But such circumstances could be used, and in some cases have been used, as a predicate to search or seize photographic equipment.

For example, two online journalists were arrested and removed from a public meeting of the Washington D.C. Taxicab Commission in 2012 for taking photographs (including video of the arrest of the first of the two reporters).[4] Both were charged

---

videotaping police, Aug. 2, 2011, http://www.poynter.org/latest-news/mediawire/141291/news-photographer-arrested-on-long-island-for-videotaping-police/; Photographers arrested during rioting, imprisoned overnight, Aug. 24, 1998 http://www.rcfp.org/browse-media-law-resources/news/photographers-arrested-during-rioting-imprisoned-overnight; Mayor apologizes to photographer for arrest at football game, Aug. 24, 1998, http://www.rcfp.org/browse-media-law-resources/news/mayor-apologizes-photographer-arrest-football-game; Charges dropped against photographers arrested in Idaho and New Mexico, Sept. 25, 1995, http://www.rcfp.org/browse-media-law-resources/news/charges-dropped-against-photographers-arrested-idaho-and-new-mexico; Police launch investigation after wrongful arrest of editor, photographer, Aug. 14, 1985, http://www.rcfp.org/ browse-media-law-resources/news/police-launch-investigation-after-wrongful-arrest-editor-photographe; Times Photographer Is Arrested on Assignment, N.Y. Times, Aug. 5, 2012, available at 2012 WLNR 16502285; Henry K. Lee, UC pays to settle photographer's suit over arrest, July 2, 2012, http://www.sfgate.com/bayarea/article/UC-pays-to-settle-photographers-suit-over-arrest-3679859.php.

[4] *See, e.g.*, Tom Sherwood, Journalists Handcuffed, Removed From Taxi Commission Meeting, June 23, 2011, http://www.nbcwashington.com/news/politics/Journalists-Handcuffed-Removed-From-Taxi-Commission-Meeting-124384719.

with disorderly conduct and "unlawful entry/remaining" by U.S. Park Police, but the government did not press charges. If the police had sought to use the search-incident-to-arrest exception in that case, it could have conducted a generalized search of the journalists' cameras and electronic notes.[5]

Similarly, a photojournalist for the *Detroit Free Press* was arrested and her camera seized while covering a police action in July 2013. At the arrest scene, the reporter captured video on her newspaper-issued iPhone. Wright was held in police custody before being released without being charged. Police returned her smartphone, but with the memory card missing. However, the video she shot of the incident, which showed Wright identifying herself as a newspaper photographer before an officer grabbed

---

html. Charges were dismissed almost immediately after the actions were widely criticized in the press. *See* Mark Seagraves, Journalists won't face charges, June 24, 2011, http://www.wjla.com/articles/2011/06/journalists-won-t-face-charges-62814.html.

[5] The Privacy Protection Act of 1980 makes it illegal for government officials to search for documents and materials that are intended for publication. 42 U.S.C. § 20000aa(b). The Act, however, contains a "suspect exception," and its restrictions on searches generally do not apply where "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate." Thus, notwithstanding the scope of the Act, if the holding in *Riley* is affirmed, journalists subjected to warrantless searches and seizures could be deprived of First and Fourth Amendment protections.

for the phone, was preserved in the camera's internal memory.[6]

Mistreatment of members of the news media by police during various Occupy Wall Street protests well illustrates this problem. Many media advocates, including *Amici*, reported numerous instances where news reporters and photojournalists were arrested along with protesters, merely for attempting to cover the events.[7] During a one-year period beginning in September 2011, more than 90 journalists were arrested in 12 U.S. cities while covering Occupy protests. *See* Josh Stearns, Tracking Journalist Arrests at Occupy Protests Around the Country, http://storify.com/jcstearns/tracking-journalist-arrests-during -the-occupy-prot (last visited Mar. 6, 2014). To allow warrantless searches of journalists' cell phones incident to such arrests raises obvious constitutional concerns.

---

[6] *See* Jim Schaefer, No charges for Detroit Free Press photographer or police officer after cell-phone seizure and arrest, Aug. 24, 2013, http://www.freep.com/article/20130823/NEWS01/308230111/detroit/free/press-photographer-mandi-wright-officer-Lamar-Penn; David Becker, Detroit Newspaper Photographer Arrested While Covering Police Action, July 16, 2013, http://petapixel.com/2013/07/16/detroit-newspaper-photographer-arrested-while-covering-police-action/.

[7] *See, e.g.*, Sara Rafsky, Protest Puts Coverage in Spotlight, N.Y. Times, Nov. 21, 2011, available at 2011 WLNR 24091906; At Occupy protests, U.S. journalists arrested, assaulted, Nov. 11, 2011, http://www.cpj.org/blog/2011/11/at-occupy-protests-us-journalists-arrested-assault.php; Josh Stearns, Citizen Journalist Arrests on the Rise at Occupy Protests, Jan. 10, 2012, http://www.freepress.net/blog/12/01/10/citizen-journalist-arrests-rise-occupy-protests.

In addition to issues facing the institutional press, the general proliferation of smart phone use by individuals to capture news events in photos and video has generated an exponential increase in "citizen journalism." Members of the public increasingly are "playing an active role in the process of collecting, reporting, analyzing and disseminating news and information."[8]

In *Glik v. Cunniffe*, 655 F.3d 78 (1st Cir. 2011), for example, a citizen was arrested after using his cell phone to photograph Boston police officers he believed were using excessive force in effectuating an arrest. Charges against him were later dropped, and Glik filed a civil action against the Boston police. In denying the individual officers' claim of qualified immunity, the First Circuit observed, "[t]he proliferation of electronic devices with video-recording capability means that many of our images of current events come from bystanders with a ready cell phone or digital camera rather than a traditional film crew, and news stories are now just as likely to be broken by a blogger at her computer as a reporter at a major newspaper." *Id.* at 84.

Likewise, in *Sharp v. Baltimore City Police*, No. 1:11-cv-02888-CCB (D. Md.), a Section 1983 action is pending based on search and seizure (and destruction) of cell phone photographs depicting the

---

[8] Shane Bowman and Chris Willis, "We Media: How Audiences are Shaping the Future of News and Information," July 2003, The Media Center at the American Press Institute, available at http://www.mediacenter/org/mediacenter/research/wemedia/.

arrest of another individual. The U.S. Department of Justice took the extraordinary step of filing a "statement of interest" supporting the plaintiff in the case, stressing that "[t]he interests animating the Fourth Amendment's prohibition against unreasonable searches and seizures are heightened when the property at issue is also protected by the First Amendment." *Id.*, DOJ Statement of Interest, at 11 (available at http://www.justice.gov/crt /about/spl/documents/Sharp_SOI_1-10-12.pdf). The DOJ filing added that "the seizure of material protected by the First Amendment is a form of prior restraint," *id.*, and that the search incident to arrest exception did not justify the search and seizure of the cell phone in these circumstances. *Id.* at 13-14. Unfortunately, arrests in similar circumstances are not uncommon.[9]

Such disturbing cases are becoming more frequent as cell phone technology proliferates and becomes more fully integrated into newsgathering activities. To the extent cell phones are treated as just another piece of property for purposes of the "search incident to arrest" exception, the frequency with which basic rights are violated will only increase over time.

---

[9] The facts of another pending civil rights action illustrate this problem (although it does not involve the search of a cell phone). In *Garcia v. Montgomery County Police*, No. 8:12-cv-03592-JFM (D. Md.), the plaintiff, an experienced photojournalist, alleges that a defendant officer illegally seized the memory card from his camera. The Department of Justice filed a Statement of Interest supporting Garcia's claims. *Id.*, DOJ Statement of Interest (available at http:// www. justice.gov/crt/about/spl/documents/garcia_SOI_3-14-13.pdf).

It therefore is necessary for this Court to clarify that a warrant is required to permit such searches. Doing so is imperative not to fashion some new right based on developing technology, but to vindicate basic guarantees of liberty as old as the Constitution itself.

B. Fourth Amendment Analysis Must Take Into Account Changes in Technology

Smart phones could not have been in the minds of the Framers when they wrote the Fourth Amendment to protect "persons, houses, papers, and effects, against unreasonable searches and seizures," U.S. Const. amend. IV, but the information contained in these devices falls squarely within the amendment's purpose. As the First Circuit recognized in *Wurie*, cell phones are mini-computers that contain information of a "highly personal nature," including "photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records." 728 F.3d at 8. "It is the kind of information one would previously have stored in one's home and that would have been off-limits to officers performing a search incident to arrest." *Id.*

This reality necessarily must inform the Court's analysis of the cases now before it, as it has long sought to assure "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). This includes drawing a line so as not to permit "technology to

erode the privacy guaranteed by the Fourth Amendment." *Id.* As this Court stressed in *Jones*, 132 S. Ct. at 951 n.3, "[w]hatever new methods of investigation may be devised, our task, *at a minimum*, is to decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment."

Past technological innovations have challenged the Court to reconcile the Framers' concern for protecting privacy with new circumstances. And while the law over time has adjusted to these changes, it has not done so immediately. In 1928, for example, this Court considered whether warrantless wiretapping violated the Fourth Amendment. At the time, it found electronic surveillance did not violate the Constitution because it was accomplished without intruding on the physical property of the defendant. The five-vote majority concluded that the Fourth Amendment "does not forbid what was done here" because "[t]he United States takes no such care of telegraph or telephone messages as of mailed sealed letters." *Olmstead v. United States*, 277 U.S. 438, 464 (1928).

Justice Brandeis, whose views ultimately prevailed, argued in dissent that constitutional principles were undermined to the extent the Court focused excessively on the method chosen for communication. He argued forcefully that constitutions must be interpreted with technological advancements in mind to preserve fundamental rights. In particular, Justice Brandeis wrote, constitutions must be designed "to approach immortality" and "our contemplation cannot only be

what has been but of what may be." *Id.* at 472-73 (Brandeis, J., dissenting).

Foreshadowing the rise of a computer-based society, he warned that:

> Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> * * *
>
> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Id. at 473-74.

Justice Brandeis concluded that, if the courts did not adapt to new realities, then constitutional principles would be "converted by precedent into impotent and lifeless formulas" and that "[r]ights declared in words might be lost in reality." *Id.* (internal quotation marks omitted).

Four decades later, the Court finally caught up with Brandeis. In *Katz v. United States*, 389 U.S.

347, 351 (1967), this Court declared that the Fourth Amendment "protects people, not places" and held that wiretapping is allowable only after a valid warrant is issued – the same as for any other search. The Court reasoned that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Id.* at 352. The decision expressly overruled *Olmstead*, replacing the previous focus on the means of communication with an appreciation of the fact of communication as the source of constitutional rights. It concluded that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied." *Id.* at 353.

The instant cases come at a seminal moment that will define the scope of constitutional protections going forward. As this Court continues to debate whether the Fourth Amendment primarily protects property or privacy, *Jones*, 132 S. Ct. at 949-52; *id.* at 958-61 (Alito, J., concurring), these cases implicate both interests: a cell phone is personal property and is an "effect" that deserves Fourth Amendment protection, and it is one that necessarily involves concerns about personal privacy. As the First Circuit observed in *Wurie*, a warrantless search of a modern cell phone "would give law enforcement automatic access to 'a virtual warehouse' of an individual's 'most intimate communications and photographs without probable cause' if the individual is subject to a custodial arrest, even for something as minor as a traffic violation." 728 F.3d at 9 (citation omitted).

Smart phones are now ubiquitous, providing capabilities that were unheard of just a few short years ago. Such mobile devices are also evolving into mobile payment devices capturing financial transactions by the owner, thus magnifying the intrusiveness of warrantless searches.[10] We are also at the dawn of the age of "wearable" devices – *e.g.*, glasses and watches and other "clothing" – that will contain even more sensitive information.[11] Whatever rule this Court fashions here will determine the level of protection accorded to these evolving technologies.

---

[10] *See* Erin F. Fonté, Overview of Mobile Payments in the United States, 32 Banking & Financial Services Policy Report No. 8, 9 (Aug. 2013) (noting that "[t]he ubiquity of mobile phones is changing the way consumers access financial services (21 percent of mobile phone owners used mobile banking within last 12 months . . .)" and that "[m]obile phones are also changing the way consumers make payments (most common use was online bill payment, and 21 percent of mobile payments users transferred money directly to another person's bank, credit card or PayPal account)").

[11] *See, e.g.*, Google Glass, Google+, https://plus.google.com/+GoogleGlass/posts#+GoogleGlass/posts (last visited Mar. 6, 2014); Gary Marshall and Kate Solomon, Apple iWatch release date, news and rumors, Feb. 17, 2014, http://www. techradar. com/us/news/ portable-devices/apple-iwatch-release-date-news-and-rumours-1131043 (describing available wearable technology and commenting on anticipated Apple iWatch); Memoto Lifelogging Camera, Memoto, https://www.kickstarter.com/projects/martinkallstrom/memoto-lifelogging-camera (last visited Mar. 6, 2014) ("The Memoto camera is a tiny camera and GPS that you clip on and wear.").

C. Fourth Amendment Protections Also Implicate First and Fifth Amendment Rights

The First, Fourth and Fifth Amendments to the United States Constitution are all predicated on protecting various aspects of individual privacy from governmental intrusion. The First Amendment guarantees that the government may not abridge freedom of speech, or of the press; the Fourth Amendment prohibits unreasonable searches or seizures, including those relating to a person's papers; and the Fifth Amendment protects individuals against government-coerced self-incrimination.

It is essential that the Fourth Amendment be scrupulously applied in cases that involve sophisticated communications technologies because of the inherent intrusion of warrantless searches on these other fundamental rights. Indeed, "[t]he Bill of Rights was fashioned against the background of knowledge that the unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus*, 367 U.S. at 729. This Court has long understood that "the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power." *Id.* at 724.

The Constitution's Framers well understood the connection between the protection of privacy and freedom of speech, for it was a part of their common routine. Thomas Jefferson and James Madison corresponded with one another over a sixty-year period, exchanging views on politics, philosophy and

constitutional theory. "Sometimes they wrote in code (later deciphered) so thoughts they exchanged would not fall into the hands of political foes." Alan Pell Crawford, Founding Fathers' Forum, Wall St. J., Feb. 2, 1995 at A16. Before the American Revolution, colonial patriots frequently concealed their authorship or circulation of literature to avoid reprisals by English-controlled courts. *Talley v. California*, 362 U.S. 60, 65 (1960). The Letters of Junius, opposing the tea tax and other oppressive measures, were written anonymously "and the identity of their author is unknown to this day." *Id.* Similarly, some of Thomas Paine's pamphlets were written under pseudonyms. *Id.* at 63 n.3. After the Revolution, the Federalist Papers, debating the merits of the Constitution, were published pseudonymously. *Id.* at 65.

Early Fourth Amendment cases emphasized the extent to which these rights are interconnected. In *Boyd v. United States*, 116 U.S. 616 (1886), for example, this Court struck down a U.S. customs law that required a person to produce in court his private books, papers or invoices or else government allegations would be taken as confessed. The Court traced the practice of issuing general warrants to the Star Chamber, which would search a suspect's papers for evidence of seditious libel. It discussed the case of John Wilkes, publisher of the North Briton, whose house was searched pursuant to a general warrant, and his books and papers indiscriminately seized to support a libel allegation. Such events "were fresh in the memories of those who achieved our independence and established our form of government." *Id.* at 625-28. *See also*

Marcus, 367 U.S. at 724-29 ("[E]ven when the device of prosecution for seditious libel replaced licensing as the principal governmental control of the press, it too was enforced with the aid of general warrants.").

This Court found that the prohibition of such "grievous abuses" and "outrage[s]" provided by the Bill of Rights represented "the true and ultimate expression of constitutional law" and constituted "the very essence of constitutional liberty and security." *Boyd*, 116 U.S. at 625-26, 630. It stressed that

> extorting the party's oath, or compelling the production of his private books and papers, to convict him of crime . . . is contrary to the principles of a free government. . . . [I]t is abhorrent to the instincts of an American. It may suit the purposes of despotic power, but it cannot abide the pure atmosphere of political liberty and personal freedom.

Id. at 631-32. In protecting such interests, the Court found that "the Fourth and Fifth Amendments run almost into each other." *Id.* at 630.

Another early case, *Ex Parte Jackson*, 96 U.S. 727, 733 (1877), established the principle that the Fourth Amendment protection for papers did not require that they be physically located in a person's home. Rather, "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be" such as "in the mail."

As in *Boyd*, the additional connection to First Amendment concerns was close to the surface. The Court discussed the attempt by President Andrew Jackson to exclude from the mails "incendiary publications" advocating the abolition of slavery in the southern states, and concluded in dictum that such a measure would "more effectually control the freedom of the press than any sedition law, however severe its penalties." *Id.* at 734 (quoting Senator Calhoun). It noted that "[l]iberty of circulating is as essential to [freedom of the press] as liberty of publishing; indeed, without the circulation, the publication would be of little value." *Id.* at 733.

Given our constitutional history, it is unreasonable to permit the warrantless search of a smart phone incident to arrest as if it were indistinguishable from any other piece of property. This Court has found that "[a] seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." *Roaden v. Kentucky*, 413 U.S. 496, 501 (1973). This principle applies with particular force to the search or seizure of expressive materials, because courts must "examine what is 'unreasonable' in the light of the values of freedom of expression." *Id.* at 504.

Just as books and films cannot be compared to "instruments of a crime, such as a pistol or a knife, or contraband or stolen goods or objects dangerous in themselves," *id.* at 502 (internal quotation marks and citation omitted), neither can a cell phone. Search and seizure of a device that serves as the repository of personal communications including

photographs, documents, texts, web browsing habits, lists of associates, and much more "calls for a higher hurdle in the evaluation of reasonableness." *Id.* at 504. *Cf. Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.").

II. THIS COURT MUST MAKE CLEAR THAT SEARCH OF A CELL OR SMART PHONE REQUIRES A WARRANT

The decisions now before this Court place the overlapping concerns of the First, Fourth, and Fifth Amendments in bold relief. In *Riley*, the California Court of Appeal simply locked onto what it viewed as the "key question" of merely "whether [Riley's] cell phone was personal property immediately associated with hi[m]" at the time of arrest. *People v. Riley*, 2013 WL 475242, at *4 (Cal. App. 4th Feb. 8, 2013) (quoting *Diaz*, 51 Cal. 4th at 93) (internal edits omitted). It thus treated the smart phone the same as any other piece of property, without regard to its storage capacity or other functions, or extent to which they implicate critical privacy interests.

In *Wurie*, by contrast, the First Circuit painstakingly explored the principles underlying the Fourth Amendment, the importance of requiring warrants for searches, and the exception for searches incident to arrest, carefully considering how modern smart phones fit within that framework. Tracing back to the pre-constitutional roots of the search warrant requirement, 728 F.3d at 3, 9, and the law's evolution to the "modern search-incident-to-arrest"

doctrine, *id.* at 3, the court rejected the government's urging "that a cell phone, like any other item carried on the person, can be thoroughly searched incident to a lawful arrest." *Id.* at 6. Such an approach, it found, "would give law enforcement broad latitude to search any electronic device seized from a person during his lawful arrest, including a laptop computer or a tablet device." *Id.* at 7.

The court noted that "[t]he storage capacity of today's cell phones is immense . . . , enough to hold about 'four million pages of documents,'" information that "by and large, [is] of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records." *Id.* at 8 (citation omitted). It added that cell phones may also provide direct access to the home through the use of remote-controlled webcams, so that "[a]t the touch of a button a cell phone search becomes a house search[.]" *Id.* at 8-9 (quoting *United States v. Flores-Lopez*, 670 F.3d 803, 806 (7th Cir. 2012)).

In short, the issues now before the Court embody Justice Brandeis' foreboding that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting). They also bring to mind the use of general warrants, by which governmental authorities would indiscriminately peruse personal papers in search of seditious writings.

The question here is not whether this Court should create new rights by divining constitutional "penumbras" and "emanations." It is whether it must preserve existing protections in the face of technological change that otherwise would allow unfettered searches to unravel guarantees for freedom of expression and against forced self-incrimination.

These interconnected rights have long been "part of the intellectual matrix within which our own constitutional fabric was shaped," *Marcus*, 367 U.S. at 729, and failure to protect them in light of changing technology would risk converting constitutional principles into "impotent and lifeless formulas" whereby "[r]ights declared in words might be lost in reality." *Olmstead*, 277 U.S. at 473-74 (Brandeis, J., dissenting).

Although the defendants in the cases below were not journalists, the issues raised by the warrantless searches of their phones incident to their arrests are of special concern to members of the press and others who use such portable electronic devices to record public events and to store private thoughts. *Amici* urge this Court to hold that a warrant must be obtained for the search of a cell phone incident to arrest because of the inherent interconnected nature of rights protected by the Fourth, First, and Fifth Amendments.

CONCLUSION

For the reasons set forth above, *Amici* respectfully ask this Court to overturn the decision of the State of California in *Riley v. State*, and affirm the decision of the First Circuit in *United States v. Wurie*.

Respectfully submitted,

Robert Corn-Revere*
Ronald G. London
Lisa B. Zycherman
DAVIS WRIGHT TREMAINE LLP
1919 Pennsylvania Ave., NW
Suite 800
Washington, DC 20006
(202) 973-4200
bobcornrevere@dwt.com

Thomas R. Burke
DAVIS WRIGHT TREMAINE LLP
505 Montgomery Street
Suite 800
San Francisco, CA 94111
(415) 276-6500

Counsel for *Amici Curiae*

* Counsel of Record

APPENDIX A

Advance Publications, Inc., directly and through its subsidiaries, publishes 18 magazines with nationwide circulation, newspapers in over 20 cities and weekly business journals in over 40 cities throughout the United States. It also owns many Internet sites and has interests in cable systems serving over 2.3 million subscribers.

American Society of Media Photographers, Inc. represents professional publication-based photographers, and is the oldest and largest organization of its kind in the world. Its roughly 7,000 members include all manner of professional photographers whose works appear in books, magazines, newspapers, web uses, corporate reports, publicity, and advertising.

With some 500 members, American Society of News Editors (ASNE) is an organization that includes directing editors of daily newspapers throughout the Americas. ASNE changed its name in April 2009 to American Society of News Editors and approved broadening its membership to editors of online news providers and academic leaders. Founded in 1922 as American Society of Newspaper Editors, ASNE is active in a number of areas of interest to top editors with priorities on improving freedom of information, diversity, readership and the credibility of newspapers.

The Association of Alternative Newsmedia (AAN) is a not-for-profit trade association for 130 alternative newspapers in North America, including weekly papers like The Village Voice and

Washington City Paper. AAN newspapers and their websites provide an editorial alternative to the mainstream press. AAN members have a total weekly circulation of seven million and a reach of over 25 million readers.

The E.W. Scripps Company is a diverse, 131-year-old media enterprise with interests in television stations, newspapers, local news and information websites and licensing and syndication. The company's portfolio of locally focused media properties includes: 19 TV stations (ten ABC affiliates, three NBC affiliates, one independent and five Spanish-language stations); daily and community newspapers in 13 markets; and the Washington-based Scripps Media Center, home of the Scripps Howard News Service.

The Investigative Reporting Workshop, a project of the School of Communication at American University, is a nonprofit, professional newsroom. The Workshop publishes in-depth stories at investigativereportingworkshop.org about government and corporate accountability, ranging widely from the environment and health to national security and the economy.

The Media Consortium is a network of the country's leading, progressive, independent media outlets. Our mission is to amplify independent media's voice, increase our collective clout, leverage our current audience and reach new ones.

The Media Law Resource Center, Inc. (MLRC) is a non-profit professional association for content providers in all media, and for their defense lawyers,

providing a wide range of resources on media and content law, as well as policy issues. These include news and analysis of legal, legislative and regulatory developments; litigation resources and practice guides; and national and international media law conferences and meetings. The MLRC also works with its membership to respond to legislative and policy proposals, and speaks to the press and public on media law and First Amendment issues. The MLRC was founded in 1980 by leading American publishers and broadcasters to assist in defending and protecting free press rights under the First Amendment.

The National Press Photographers Association (NPPA) is the nation's leading professional organization for photojournalists. NPPA's membership includes photographers, members of the press generally, and citizen journalists. As a nationally recognized authority on the right to photograph and record audio-visual images, the NPPA advocates for visual journalists in disputes involving interference with that right.

The New York Times Company is the publisher of *The New York Times*, *The Boston Globe*, and *International Herald Tribune* and operates such leading news websites as nytimes.com and bostonglobe.com.

Newspaper Association of America (NAA) is a nonprofit organization representing the interests of more than 2,000 newspapers in the United States and Canada. NAA members account for nearly 90% of the daily newspaper circulation in the United States and a wide range of non-daily newspapers.

The Association focuses on the major issues that affect today's newspaper industry, including protecting the ability of the media to provide the public with news and information on matters of public concern.

Online News Association (ONA) is the world's largest association of online journalists. ONA's mission is to inspire innovation and excellence among journalists to better serve the public. ONA's more than 2,000 members include news writers, producers, designers, editors, bloggers, technologists, photographers, academics, students and others who produce news for the Internet or other digital delivery systems. ONA hosts the annual Online News Association conference and administers the Online Journalism Awards. ONA is dedicated to advancing the interests of digital journalists and the public generally by encouraging editorial integrity and independence, journalistic excellence and freedom of expression and access.

The Reporters Committee for Freedom of the Press is a voluntary, unincorporated association of reporters and editors that works to defend the First Amendment rights and freedom of information interests of the news media. The Reporters Committee has provided representation, guidance and research in First Amendment and Freedom of Information Act litigation since 1970.

Student Press Law Center (SPLC) is a nonprofit, nonpartisan organization which, since 1974, has been the nation's only legal assistance agency devoted exclusively to educating high school and college journalists about the rights and

responsibilities embodied in the First Amendment to the Constitution of the United States. SPLC provides free legal assistance, information and educational materials for student journalists on a variety of legal topics.

APPENDIX B

Richard A. Bernstein
Sabin, Bermant &
Gould LLP
Four Times Square
New York, NY 10036
Counsel for Advance Publications, Inc.

Victor S. Perlman
American Society of
Media Photographers
150 North 2nd St.
Philadelphia, PA 19106

Kevin M. Goldberg
Fletcher Heald &
Hildreth
1300 N. 17th St.
11th Fl.
Arlington, VA 22209
Counsel for American Soc. of News Editors and Assn. of Alternative News Media

David M. Giles
Vice President/Deputy
General Counsel
The E.W. Scripps Co.
312 Walnut St.
Suite 2800
Cincinnati, OH 45202

Lynne Perri
Managing Editor
Investigative Reporting
Workshop
School of Communication/
American University
4400 Mass. Ave. NW
Washington, DC 20016

Sandra S. Baron
Media Law Resource Ctr.
520 Eighth Avenue
North Tower
20th Floor
New York, NY 10018

Mickey Osterreicher
National Press
Photographers Assn.
1100 M&T Center
3 Fountain Plaza
Buffalo, NY 14203

David McCraw
V.P./Assistant General
Counsel
The New York Times
Company
620 Eighth Avenue
New York, NY 10018

Kurt Wimmer
Covington & Burling LLP
1201 Pennsylvania Ave., NW
Washington, DC 20004
Counsel for the Newspaper Association of America

Jonathan D. Hart
Dow Lohnes PLLC
1200 New Hampshire Ave., NW
Washington, DC 20036
Counsel for Online News Association

Bruce D. Brown
Gregg P. Leslie
The Reporters Committee for Freedom of the Press
1101 Wilson Blvd.
Suite 1100
Arlington, VA 22209

Frank D. LoMonte
Student Press Law Center
1101 Wilson Blvd.
Suite 1100
Arlington, VA 22209